Risks of Ubiquitous Information and Communication Technologies:

How Individuals Perceive, Cause, and Seek to Mitigate Them

Thesis
presented to the Faculty of Arts
of
the University of Zurich
for the degree of Doctor of Philosophy

by
Stephanie Moser Froidevaux
of Herbligen BE

Accepted in the fall semester 2010 on the
recommendation of Prof. Dr. Hans-Joachim Mosler,
Prof. Dr. Heinz Gutscher, and Prof. Dr. Ruth Kaufmann-Hayoz

Zurich, 2011

Acknowledgements

This thesis would not exist without the support of numerous persons and institutions, to whom I would like to express my gratitude. The work for this thesis was part of the project 'Cooperative Assessment and Communication of Systemic Risks of Ubiquitous Information and Communication Technologies (AACCrisk)'. This project was funded by the German Federal Ministry for Education and Research (BMBF), within the research program Socio-Ecological Research (SÖF), under the thematic topic 'Strategies for Coping with Systemic Risks'. Funds for the completion of the thesis were further provided by the 'Janggen Pöhn Stiftung' (St.Gallen) and the University of Zurich, to whom I am much indebted.

The AACCrisk project was conducted in cooperation with the partner institutions 'Ecolog Institut' (Hannover) and 'Sinus Sociovision' (Heidelberg). I would like to thank the personnel of these institutions, particularly Dr. H.-Peter Neitzke and Dr. Silke Kleinhückelkotten, for their interesting and informative collaboration.

I owe a debt of gratitude to my supervisors from the University of Zurich. From the beginning, Prof. Hans-Joachim Mosler supported my work with an ideal mix of high expectations and professional as well as motivational support. I thank Prof. Heinz Gutscher for his flexibility, openness and participation.

During the five years of work on this thesis, the 'Interdisciplinary Center for General Ecology (IKAOE)' at the University of Bern has provided me with an inspiring ambiance and place of work, where I received professional and humane assistance. Primarily, I owe thanks to my supervisor and head of the IKAOE Prof. Ruth Kaufmann-Hayoz. With her unshakable optimism, she believed in the success of this work from the very beginning. In numerous discussions, she helped to solve problems and questions, and, thanks to her review and precision, the work gained in consistency. Moreover, I would like to sincerely thank Dr. Susanne Bruppacher for her preliminary conceptual work in the AACCrisk project, and for her confidence in rendering 'her' project to me. She always found time for my scientific or motivational problems.

My thanks go further to the team of the IKAOE. The vivid and interesting interdisciplinary discussions significantly broadened my scientific horizon. I am particularly indebted to my colleagues Lisa Lauper, Maja Fischer, Matthias Mueller, Stefan Groesser, and Fred DeSimoni for their support, discussions, feedback, and proofreading. Philippe Cosi always provided IT emergency aid, and Kathrin Wegmueller supplied me with all the scientific literature I needed.

Last but not least, I owe special gratitude to my family. My mother-in-law Bettina Froidevaux had immense patience in providing me with language support. Every evening, my two sons Leander and Julian made sure that I did not lose ground in the 'scientific spheres'. My husband Cédric released me from everyday burdens and showed a great deal of understanding for evenings and weekends occupied with work. Thanks so much to all of you!

Table of Contents

List of Figures and Tables

Summary

Information and communication technologies (ICT) are increasingly shaping the daily lives of people in Western societies. Current technological progress can be characterized by an increased power of technological components, combined with a continuous decrease in their size. These advances allow for the embedding of ICT components in commodities, and for their interconnection with each other and with technologies transmitting information, such as the Internet or mobile phones. This new generation of so-called 'smart' technologies is meant to support people in their accomplishment of everyday tasks, invisibly, automatically, and ubiquitously.

This trend in the direction of life settings shaped by ubiquitous ICT bears, apart from potential benefits, several risks. However, as yet, these risks have primarily been discussed from a technological, and expert perspective. The view of ordinary citizens, as well as the potential relevance of people's behavior with respect to the risks of ubiquitous ICT, has only rarely been the subject of research. Thus, the overall objective of this thesis was to gain a better understanding of the relevance of individual behavior in terms of the risks of ubiquitous ICT. Better insights into the human dimensions of the risks of ubiquitous ICT are considered to be a precondition for the identification of attachment points for policies that lower the risks in development and use of ubiquitous ICT.

In a first step, human involvement was regarded from the perspective of people potentially 'concerned' by the risks of ubiquitous ICT. From this perspective, relevant research questions concerned changes which people expect from ubiquitous ICT, the trains of thought upon which people base their expectations, and different risk components affecting subjective risk judgments.

Second, humans were seen in the role of 'managers' coping with the risks of ubiquitous ICT. In this regard, questions of interest were related to potential individual protective behaviors, the relationship between individual threat appraisal and the development of an intention to protect, additional predictors impacting protective intentions, and potential progressions of individual protective behavior over time and under changing external impacts.

The third perspective of human involvement focused on humans as 'producers' of risks of ubiquitous ICT. Of particular interest were questions concerning the emergence of reactance and non-protective reactions, as well as potential progressions of non-protective behavior over time and under changing external impacts.

To address these questions, an iterative procedure was chosen which alternated between theoretical consolidation and three empirical and conceptual studies. In the first study, carried out in 2006, eleven qualitative interviews were conducted in Berlin, Germany. A visual interview technique, named 'Cognitive Mapping' was adapted and applied in order to elicit the mental models

of the interviewees. The mental models explored concerned anticipated changes in the outpatient health sector evoked by the implementation of ubiquitous ICT.

The insights gained in study 1 fostered the need for a better understanding of people's motivation to take protective action. The key concepts identified in study 1 supported the choice of the protection motivation theory (PMT) as well as further psychological risk concepts as theoretical foundations for the second study. Based on these theoretical concepts, a model was hypothesized explaining the emergence of protective and non-protective intentions. The model was tested with structural equation modeling. Data stem from standardized interviews of a representative sample (*N*=5030). This investigation arose from cooperation with our partner institutions and was implemented in 2007 in Germany.

The results from study 2 gave rise to open questions regarding potential reciprocities in the model structure and dynamic progressions of the variable levels over time. These issues stimulated interest in control theoretical frameworks, which understand individual risk perception and protective behavior as embedded in a reciprocal, self-regulating system. In the third study, different control-theoretical frameworks were integrated in a mathematical model with the help of 'System Dynamics' computer modeling. This computer model allowed for the simulation of protective behavior over time and under changing external impacts. To facilitate the integration, the model was substantiated using the example of security behavior regarding current ICT.

Being concerned implies, in a first phase, the perception and appraisal of risks. Study 1 revealed that the interviewees predominantly expected undesired changes due to the implementation of ubiquitous ICT in the outpatient health sector. The key concepts identified encompassed several personal and societal consequences that the interviewees feared, such as the loss of individual control, temporal and financial losses, enhanced abuse and defectiveness of data, increased discrimination against people who are unwilling or unable to use ubiquitous ICT, as well as increased general incapacity and public surveillance. Conversely, only a few benefits were expected from ubiquitous ICT and these only for individual users, such as financial savings, as well as gains in time and control. The main drivers of the undesired consequences were seen as the exchange of data among the providers of services based on ubiquitous ICT, and the general acceptance and diffusion of the technologies in society.

The quantitative model test in study 2 revealed significant regression weights of the individual's own susceptibility and negative affect evoked by ubiquitous ICT explaining perceived threat. Furthermore, negative affect was significantly negatively related to previous use of ICT, as well as to the trust that precautions would be taken by the institutions responsible.

Based on the dynamic model conceptualized in study 3, it may be assumed that previously undertaken security measures may be a further factor affecting the perceived threat.

In order to counteract the risks of ubiquitous ICT, interviewees of study 1 mentioned the search for information on the new technologies and their risks, political protest, renouncing the use of ubiquitous ICT, as well as attempting to avoid the registration of personal data. The quantitative model test in study 2 disclosed significant positive regression weights from perceived threat on the intention to search for information and the intention to engage politically. This model test revealed further significant positive relations between the two protective intentions and the appraisal of the corresponding coping efficacies, as well as negative relations between the intentions and negative emotions felt. The progression of the level of protective behavior over time was simulated in study 3 with the help of the computer model. This procedure led to the assumption that highly valued protective principles and high perceived coping efficacy might be preconditions for an appropriate increase in individual protective behaviors to perceived hazards.

Risks of ubiquitous ICT emerge not least due to inopportune individual behaviors, for example in the form of reactance responses as referred to by the interviewees of study 1. Examples of reactance mentioned were boycotting of technological services and their providers, manipulation of data registration, and incorrect or minimalist use of the technological services. Such responses were mentioned as being the last options for reaction if individuals are forced to use ubiquitous ICT due to a lack of technology-free alternatives, or legal regulations.
Risks may further emerge if individuals fail to implement protective measures and relapse in terms of non-protective responses, such as, overstrain or helplessness. The model test in study 2 revealed non-protective reactions to be significantly related to high perceived threat, high negative affect and low perceived coping efficacies. Based on the dynamic model simulation in study 3, it can be assumed that in such a case, an individual reduces the significance of his or her protective principles. Thereby, the risk tolerance of the individual increases and he or she becomes indifferent to situational risk cues.

From the findings of this thesis, three main implications can be drawn for precautions against the risks of ubiquitous ICT. First, efforts to preserve high degrees of individual control and freedom of choice have to be increased. People have to be allowed and enabled to decide on their own when and which services and applications of ubiquitous ICT they want to use and which not. Only then can reactance responses be avoided. Second, individual overstrain regarding the risks of ubiquitous ICT has to be prevented. For risk communication, this implies also communicating individual coping options, thus avoiding overwhelming affective reactions. Third, public trust in ubiquitous ICT should be enhanced. In addition to the two demands mentioned above, this encompasses the requirement to launch only well-engineered products, with observable

and effective advantages for users, as well as to attach the highest priority to the protection of personal data and privacy.

Zusammenfassung

Informations- und Kommunikationstechnologien (IKT) prägen zunehmend das Alltagsleben vieler Menschen, insbesondere in der industrialisierten Welt. Rasante technologische Fortschritte ermöglichen kommenden IKT Generationen zusätzliche Möglichkeiten: Durch die ansteigende Leistungsfähigkeit der technologischen Komponenten, einhergehend mit einer ständigen Verringerung deren Grösse, können IKT Anwendungen vermehrt in Alltagsgegenstände eingebettet, sowie gegenseitig vernetzt werden. Sogenannt ‚intelligente' Gegenstände sollen in Zukunft die Anwender und Anwenderinnen möglichst unsichtbar, automatisiert und allgegenwärtig bei der Bewältigung ihres Alltags unterstützen.

Der Trend hin zu Lebenswelten, welche mit vernetzten, allgegenwärtigen IKT durchdrungen sind, birgt nebst möglichen Vorteilen jedoch auch verschiedene Risiken. Diese wurden bisher hauptsächlich aus technologischer Sicht und von Experten thematisiert. Die Sichtweise der breiten Bevölkerung, sowie die mögliche Relevanz individuellen Handelns in Hinblick auf die Risiken allgegenwärtiger IKT, wurde bisher kaum erforscht. Das übergeordnete Ziel der vorliegenden Arbeit war es deshalb, verschiedene Aspekte menschlicher Beteiligung in Bezug auf die Risiken allgegenwärtiger IKT zu beleuchten. Ein besseres Verständnis der Rolle des Menschen bezüglich der Risiken allgegenwärtiger IKT ist eine Voraussetzung für die Identifikation von Ansatzpunkten für präventive Massnahmen, um allfälligen Risiken entgegen wirken zu können.
Als Erstes wurde der Mensch in der Rolle des durch Risiken allgegenwärtiger IKT ‚Betroffenen' betrachtet. Aus dieser Perspektive stellten sich die Fragen, welche Veränderungen Personen aufgrund der Verbreitung allgegenwärtiger IKT erwarten, aufgrund welcher Gedankengänge die Personen zu diesen Prognosen kommen und welche Risikomerkmale die Höhe der subjektiven Risikourteile bestimmen.
Ein zweiter Aspekt umfasste den Menschen in der Rolle des ‚Bewältigenden' der Risiken allgegenwärtiger IKT. Hierzu stellten sich die Fragen nach möglichen Schutzhandlungen, nach dem Zusammenhang zwischen der Bewertung der Risiken allgegenwärtiger IKT und dem Zustandekommen von Schutzintentionen, nach zusätzlichen Prädiktoren dieser Intentionen, sowie nach möglichen Entwicklungsverläufen von Schutzhandlungen über die Zeit und unter sich verändernden Einflussfaktoren.
Als dritter Aspekt wurde der Mensch in der Rolle des ‚Verursachers' möglicher Risiken betrachtet. Hierzu interessierten insbesondere die Fragen, warum reaktante Reaktionen auf die Technologien entstehen könnten, warum Personen mögliche Schutzhandlungen unterlassen, und wie sich dieses Verhalten über die Zeit unter Berücksichtigung verschiedener Einflussfaktoren entwickeln könnte.

Zur Untersuchung dieser Fragen wurde ein iteratives Vorgehen gewählt, welches zwischen theoretischer Vertiefung und drei empirischen und konzeptuellen Einzelstudien alternierte: In der ersten Studie wurden mit Hilfe von elf qualitativen Interviews, welche im Herbst 2006 in Deutschland durchgeführt wurden, die mentalen Modelle von Personen exploriert. Die erforschten mentalen Modelle umfassten erwartete Veränderungen im Gesundheitsbereich, verursacht durch das Aufkommen allgegenwärtiger IKT. Zur Erhebung der Interviews wurde die visuelle Interviewtechnik ‚Cognitive Mapping' adaptiert.
Die Erkenntnisse aus dieser ersten Studie führten zur Einsicht, dass ein besseres Verständnis nötig ist, warum Personen mögliche Schutzhandlungen ausführen oder unterlassen. Die in der ersten Studie identifizierten Schlüsselkonzepte unterstützten die Wahl der Schutz-Motivations-Theorie als theoretische Grundlage, sowie weiterer theoretischer Risikokonstrukte für die nachfolgende zweite Studie. Basierend auf diesen Theorien wurde ein Modell zur Erklärung protektiver und non-protektiver Intentionen erstellt und mittels Strukturgleichungsmodellierung überprüft. Die Daten hierzu stammten aus einer Befragung, welche in Kooperation mit Partnerinstitutionen im Jahr 2007 an einer repräsentativen Stichprobe (N = 5030) in Deutschland durchgeführt wurde.
Die Resultate der zweiten Studie liessen allerdings Fragen nach möglichen reziproken Beziehungen zwischen den einzelnen Variablen, sowie nach deren dynamischer Entwicklung über die Zeit offen. Diese Einsichten stimulierten das Interesse an kontrolltheoretischen Ansätzen, welche Risikowahrnehmung und Schutzverhalten als sich selbst regulierendes System auffassen. Verschiedene kontrolltheoretische Ansätze wurden in der dritten Studie mit Hilfe von systemdynamischer Computermodellierung in ein mathematisches Modell transferiert. Dieses Computermodell erlaubte die Simulation von Schutzverhalten über die Zeit und unter sich verändernden externen Bedingungen. Zur Konkretisierung wurde dieses Modell am Beispiel von Sicherheitsverhalten in Bezug auf aktuelle IKT erstellt.

Betroffenheit impliziert in einem ersten Schritt die Wahrnehmung, respektive Bewertung, der Risiken. Studie 1 zeigte auf, dass die Befragten überwiegend unerwünschte Veränderungen durch die Verbreitung allgegenwärtiger IKT im Gesundheitsbereich befürchteten. Die identifizierten Schlüsselkonzepte umfassten verschiedene erwartete negative persönliche und soziale Folgen, wie den Verlust der eigenen Kontrolle, zeitliche und finanzielle Einbussen, zunehmenden Missbrauch und vermehrte Fehleranfälligkeit der Daten, erhöhte Diskriminierung von Personen, welche allgegenwärtige IKT nicht nutzen können oder wollen, sowie eine generelle Entmündigung der Bevölkerung und zunehmende staatliche Überwachung. Demgegenüber wurden nur wenige Vorteile für einzelne Nutzende der Technologien gesehen, wie finanzielle Einsparungen, Zeit- und Kontrollgewinne. Als Hauptursachen der unerwünschten Veränderungen wurde die allgemeine Akzeptanz und Verbreitung der Technologien in der Gesellschaft, sowie die Weiter-

gabe und der Austausch von Daten durch die Anbieter von auf allgegenwärtige IKT gestützten Diensten gesehen.
Die quantitative Modellprüfung in Studie 2 ergab signifikante Regressionsgewichte für die Einschätzung der eigenen Betroffenheit und die Höhe des durch die Technologien ausgelösten negativen Affekts auf die Einschätzung der Höhe der Risiken allgegenwärtiger IKT. Der empfundene Affekt seinerseits korrelierte negativ mit der Höhe des Vertrauens in für Risikoprävention verantwortliche Institutionen und der Höhe der bisherigen Nutzung von IKT.
Aufgrund der Konzeption des dynamischen Modells in Studie 3 lässt sich zudem vermuten, dass die bereits unternommenen individuellen Sicherheitsvorkehrungen als weiterer Faktor die Höhe der Risikobewertung beeinflussen.

Um den antizipierten Risiken allgegenwärtiger IKT entgegen zu wirken, nannten die Befragten in der ersten qualitativen Studie als Beispiele möglicher Schutzhandlungen die Suche nach Informationen zu den Technologien und deren Risiken, politischen Protest, den Verzicht auf die Nutzung allgegenwärtiger IKT und den Versuch, die Registrierung persönlicher Daten zu vermeiden. Der quantitative Modelltest in Studie 2 ergab einen signifikanten Zusammenhang zwischen der Höhe der Risikobewertung, sowie den Intentionen, Informationen zu suchen und sich politisch zu engagieren. Die Modellauswertung ergab zudem signifikante Regressionsgewichte von der Höhe der Einschätzung der Bewältigungsmöglichkeiten auf die beiden untersuchten Schutzintentionen, sowie negative Zusammenhänge zwischen den Intentionen und dem empfundenen negativen Affekt. In Studie 3 wurde mit Hilfe des dynamischen Computermodells die Entwicklung der Höhe von Schutzverhalten über die Zeit simuliert. Dieses Vorgehen ergab, dass sowohl eine hohe Wertschätzung bedrohter Prinzipien, wie auch eine hohe Einschätzung der eigenen Bewältigungsmöglichkeiten Vorbedingungen für eine adäquate Anpassung des Schutzverhaltens an eine wahrgenommene Erhöhungen des Risikolevels sind.

Risiken allgegenwärtiger IKT entstehen nicht zuletzt durch unadäquate individuelle Handlungen. Ein Beispiel hierzu sind reaktante Reaktionen, wie sie von den Befragten in Studie 1 als Möglichkeiten genannt wurden. Genannte Beispiele hierzu sind der Boykott von technologischen Diensten, respektive deren Anbietern, Manipulation der Datenerhebung, sowie inkorrekter oder minimalistischer Gebrauch der technologischen Dienste. Diese Massnahmen wurden von den Befragten erwägt, falls ein freiwilliger Verzicht auf die Dienste allgegenwärtiger IKT mangels gesetzlicher Bestimmungen oder fehlender technikfreier Alternativen nicht mehr möglich wäre.
Risiken, insbesondere für die Betroffenen selber, entstehen auch, wenn mögliche Schutzhandlungen nicht ausgeführt werden und die Person in non-protektive Reaktionen verfällt, wie beispielsweise Überforderung und Hilflosigkeit. Wie die quantitative Modellauswertung in Studie 2 ergab, stehen non-protektive Reaktionen in Zusammenhang mit einer hohen Risikobewertung,

hohem Empfinden von negativem Affekt, kombiniert mit einer tiefen Einschätzung der eigenen Bewältigungsmöglichkeiten. Aufgrund der dynamischen Modellsimulation in Studie 3 kann angenommen werden, dass in einem solchen Fall ein Individuum die Gewichtung der schützenswerten Prinzipien verringert. Dadurch steigt die Risikotoleranz der Person und diese wird immun gegenüber Risikohinweisen aus dem Umfeld.

Aus der vorliegenden Arbeit lassen sich drei Hauptimplikationen für die Prävention von Risiken allgegenwärtiger IKT ableiten. Erstens muss der Erhalt möglichst hoher individueller Kontroll- und Wahlmöglichkeiten angestrebt werden. Personen müssen selber entscheiden können ob, wann und welche von allgegenwärtigen IKT unterstützter Dienste und Anwendungen sie nutzen möchten und welche nicht. Nur so können reaktante Reaktionen auf die neuen Technologien vermieden werden. Zweitens muss individuelle Überforderung angesichts der Risiken der Technologien vermieden werden. Dies bedeutet beispielsweise für die Kommunikation von Risiken, dass gleichzeitig Möglichkeiten der individuellen Bewältigung aufgezeigt, und überbordende affektive Reaktionen vermieden werden sollten. Drittens sollte das öffentliche Vertrauen in die Technologien gestärkt werden. Nebst den beiden oben genannten Punkten gehört hierzu die Forderung, dass nur ausgereifte technologische Produkte zur Anwendung kommen, welche einen sichtbaren und effektiven Nutzen bringen, sowie dass der Sicherheit von Daten und dem Schutz der Privatsphäre der Nutzenden höchste Priorität beigemessen wird.

Chapter 1:
An Overview of the Thesis

1. Introduction

Information and communication technologies (ICT) are increasingly pervading our daily lives, fundamentally changing our living environments. This is especially the case for industrialized countries such as Switzerland and Germany, where this thesis can be situated. The technological progress of sensors and processors becoming smaller and cheaper is still accelerating (Mattern, 2003). These trends allow for the increasing integration of ICT components within commodity items. Such so-called 'smart' devices are enabled to interact with each other or the users by exchanging information, and to sensitively react to their environment. These technological opportunities evoke visions that have been called 'ubiquitous computing' (Weiser, 1991) - living environments pervaded with omnipresent ICT, which allow information and communication anywhere and anytime (Neitzke, et al., 2008). Following the precaution principle, potential negative consequences of ubiquitous ICT, i.e., their risks, should be investigated early on (Som, Hilty, & Ruddy, 2004). Potential risks of ubiquitous ICT have been discussed from the viewpoint of experts (e.g., by Hilty, Bruinink, Köhler, & Som, 2003; Mattern, 2003), however mostly only against a technical background. Empirical investigations from the viewpoint of ordinary citizens are rare (BSI, 2006; Hilty, et al., 2003; Neitzke, et al., 2008). Thus, the human dimensions of the risks of ubiquitous ICT have largely been neglected. The objective of this thesis was to address this gap. The aim was to achieve a better understanding of the human factor within the production and mitigation of the risks of ubiquitous ICT. To do this, psychological components of the subjective perception of the threats of ubiquitous ICT were investigated among the population, and related to potential precautionary intentions, and non-protective reactions, respectively. Knowledge about individual factors impacting the mitigation of the risks of ubiquitous ICT were considered to be a precondition for the formulation of recommendations on policies supporting protection.

The present chapter provides an overview of the thesis. Section two of the chapter presents ongoing and future technological trends in ICT. Section three describes risks of ubiquitous ICT discussed in the scientific literature in terms of an individual focus. Section four presents an overview of the concrete goals of the thesis and research questions. Section five illuminates the context in which the thesis emerged. Section six introduces the general procedure applied, and finally, section seven presents the psychological risk theories relevant to this thesis.

2. An increasingly technologized environment

In Western society, the absence of information and communication technologies is hardly imaginable. In the year 2007, 89% of Swiss households had one, 49% even two mobile phones. Fur-

Furthermore, 74% of households had Internet access, 79% of the households had one and 30% had more than one personal computer (BFS, 2010). A similar technological dispersion can be found in Germany, where the 80% threshold of households with a mobile phone was exceeded in 2006 (Statistisches Bundesamt Deutschland, 2007). In 2007, 65% of German households had Internet access, and 73% had a personal computer (Czaijka & Mohr, 2008).

After the era of 'mainframe computing', in which one processor was shared by many users, and the era of 'personal computing', which can be summed up as one computer per person, in 2012, we will presumably enter the next wave in computer history (Hilty, et al., 2003; Neitzke, et al., 2008). This next paradigm shift to 'ubiquitous computing' can be characterized as one person using a multitude of computers. According to estimations by IBM, about one billion people around the world will be using more than a trillion networked devices in the coming years. For the industrialized countries, this represents, on average, 1000 'smart objects' per person (Hilty, 2005). This trend is the result of the rapid technological progress in the development of ICT. Forty years ago, Moore noticed that the power of microprocessors roughly doubled every eighteen months (Moore, 1965). This estimation has proved to be valid up to now and is bound to continue for several more years (G. E. Moore, 2003). Other ICT components, such as the rate of data transmission or wired and wireless networks, have been experiencing a similar increase in power (BSI, 2006).

The continuing increase in capacity of ICT components has led to a decrease in their size and costs (Mattern, 2003). This trend allows for an increased embedding of ICT components into technological and non-technological devices (Hilty, 2005), such as packaging, clothing, household appliances or toys. Further new qualities of ubiquitous ICT are its context awareness and increased interconnectedness. Devices are constructed to sense information from their computational or physical environment (e.g. identity or location), to recognize activity, as well as to create a representation of their context (Abowd & Mynatt, 2000). This allows for automated, adaptive, and personalized responses (Mattern, 2003).

The vision of a technologized environment in which 'invisible' ICT provides services and information anywhere and anytime to support people in accomplishing their daily routines, has been named 'ubiquitous computing' (Weiser, 1991), 'pervasive computing' (Hilty, et al., 2003), 'the Internet of things' (Mattern & Floerkemeier, 2010; Schoenberger, 2002), or 'AACC' (anytime anywhere communication and computing) (Neitzke, et al., 2008). According to Greenfield (2006), ubiquitous computing is not a particular kind of hardware or software, but should rather be considered as describing a set of circumstances, situations or settings shaped by ubiquitous ICT. Such settings, in terms of what individuals' lives may look like, have been described by Neitzke and colleagues (Neitzke, Behrendt, & Osterhoff, 2006). Examples of such settings are, for example, smart homes, ICT-supported health care applications, intelligent traffic systems, or ICT-supported work surroundings:

Smart homes: Completely digitalized building service engineering automatically regulates supply and removal of water, heat, light, and electronic devices (Hilty, et al., 2003; Rohrschacher, 2002). The services can be operated by a central server, or from outside, such as by smart grids. A popular extension of a smart home is a smart refrigerator, which recognizes its contents and automatically orders missing food items from the retailer.

E-health: Apart from medicinal technology, ICT will increasingly be used for communication, e.g., in the form of electronic patient records, as well as for health monitoring and support, e.g., in the form of home care supported by ubiquitous ICT (Ahern, 2007; S. Brown, Hine, Sixsmith, & Garner, 2004; Müller, et al., 2003; Neuhauser & Kreps, 2003; Tan, 2005).

Intelligent traffic systems: The capacity of public transport systems may be optimized by means of ICT-supported fare management systems. Individual traffic fluidity and security may be enhanced with intelligent control systems, and adaptive drive systems may decrease energy consumption and pollutant emissions (Herrtwich, 2003; Hilty, et al., 2003; Linneweber, 2007).

Workspace: Virtual teams and rooms allow for time- and location-independent work-fostering telework (Hilty, et al., 2003; Jessup & Robey, 2002).

It is estimated that ubiquitous ICT infrastructure will have pervaded all aspects of daily life within ten years (Neitzke, et al., 2008). First steps in this direction have already been implemented. Several ubiquitous ICT components are now viable, some of which have already reached affordability, such as RFID tags, as well as mobile phones with wireless Internet access (BSI, 2006; Neitzke, et al., 2008). However, ubiquitous computing will attain dimensions that far exceed current ranges of application and dispersal (Hilty, et al., 2003).
Drivers of the diffusion are expectancies of enhanced convenience and safety, lower administrative costs, savings of natural resources and energy, or eased monitoring of health states or natural reserves. Ubiquitous ICT are further meant to offer an immense market potential for the IT and telecommunication industries (Greenfield, 2006; Hilty, et al., 2006; ITU, 2005, 2006; Mattern, 2005).
But, obviously, there may be another side of the coin; undesired changes, i.e., risks of ubiquitous ICT may have to be expected as well. The next section introduces the notion of potential risks of ubiquitous ICT in relation to different roles humans may play in their emergence and mitigation.

3. Risks of ubiquitous ICT with respect to differences in human involvement

Human involvement plays a crucial role in relation to risks of artificial environments shaped by technological progress. This human impact can be regarded from three different perspectives. First, humans are the producers and users of the technologies and thus, at least indirectly, the initiators of technological risks. Second, humans are those primarily exposed to the risks, i.e., the victims. Third, humans can be considered to be risk regulators or managers, who learn to handle and master the changed circumstances (Böhm, 2008; Kruse, 1981). In the next subchapter, to enable better consistency with the subsequent order of the thesis, human exposure to the risks of ubiquitous ICT is addressed first, followed by considerations regarding individual risk handling and risk causation.

3.1. Aspects of human susceptibility to the risks of ubiquitous ICT

Besides potential impacts on the natural environment (cf. section 3.3.), humans, or at least some of them, will be most concerned by the negative aspects of the progress of ubiquitous ICT. It is expected that risks and benefits will not be equally distributed in society. The so-called 'digital divide' may spread, increasing advantages for people who can benefit from new technologies, while others with lesser IT access and skills will be left behind (Lyon, 2001; Viswanath & Kreuter, 2007). Potential losers due to ubiquitous ICT may be elderly people, political minorities, IT skeptics, marginal groups, persons with 'unorthodox' biographies, small-sized companies as well as the retail industry (BSI, 2006).

Regarding personal risks, experts fear that privacy and data protection rights will be undermined and that surveillance options will increase (Beresford & Stajano, 2003; Friedermann, Vildjiounaite, Punie, & Wright, 2006; Greenfield, 2006; Stajano, 2003). Paradoxically, individuals will mostly be unaware of what data is collected by whom, of who will have access to these data, and of what other data they will be combined with (Hubig, 2003; Lyon, 2001). Further concerns are potential restrictions on the freedom of choice of consumers or patients (Hilty, Som, & Köhler, 2004; Stone, 2003).

However, the question of how the risks of ubiquitous ICT that are being discussed among experts are also appraised by laypersons has mainly been neglected so far. It is known that risk judgments of laypersons differ from those of experts (Kemp, 1993). Experts typically use a quantitative definition of risk whereby the potential damage is multiplied by the expectancy of occurrence (Günther, 1998). Non-experts, however, construe their risk judgments according to further risk characteristics, such as personal susceptibility, lacking control options, affective sensa-

tions or the novelty of a phenomenon (Slovic, 1987, 1992; Slovic, Fischhoff, & Lichtenstein, 1982).

Studies looking at laypersons' risk judgments regarding ubiquitous ICT are rare. In a multistage risk detection and rating survey about ubiquitous computing, laypersons' greatest concerns were found to relate to data security, functionality and privacy issues (Behrendt, Kleinhückelkotten, Neitzke, & Wegner, 2007; Neitzke, et al., 2008).

However, for a better understanding of the victims' perspective, further research is needed, exploring the aspects of the appraisal of risks of ubiquitous ICT from the viewpoint of those people who are potentially concerned.

3.2. Individual handling of risks of ubiquitous ICT

Humans do not have to remain in the role of the victim. Risk mitigation might take place on an institutional level in the form of risk regulation and governance (Renn, 2005, 2008). It must be anticipated, however, that legislation may lag behind technological development, so that the enhanced complexity of ubiquitous ICT settings will impair control and blur responsibilities (Hilty, et al., 2004).

Thus, technological handling on an individual level may play a crucial role in risk prevention and mitigation. There are theoretical frameworks explaining antecedents of individual protective behavior (cf. section 6.2.), although, to the best of my knowledge, they have not so far been adapted to the threats of ubiquitous ICT. Thus, in order to better understand the way in which a competent, intentional and self-determined handling of ubiquitous ICT could be supported, research is required that investigates the relationship between the individual perception of risks of ubiquitous ICT and potential protective reactions.

3.3. Humans causing risks of ubiquitous ICT

Unlike with natural hazards, human actions are the main cause of the emergence of technological risks such as those of ubiquitous computing. Harm from ICT may potentially be caused in different ways. A first way is the intended, abusive use of the technologies in the form of intentional destruction or detrimental misuse (Stanton, Stam, Paul, & Jolton, 2005). Concerning ubiquitous ICT, new forms of computer criminology may occur with coincidentally inexplicit legal positions (Hilty, et al., 2003).

Second, harm may emerge even under the condition that all users behave (from the technological point of view) in an intended way (Neitzke, et al., 2008): in this case, the production and operation of ubiquitous ICT may result in a growing need for raw materials and energy (Hilty, 2005). The integration of the ICT components in commodity items may impede professional

waste management and recycling of the different materials (Poldervaart, 2009; Waeger, Eugster, Hilty, & Som, 2005). Additionally, non-ionic radiation exposure may increase (Hilty, et al., 2003; Hilty, et al., 2004).

Third, causes of risks of ICT may emerge from naive mistakes and the omission of security measures (Leach, 2003; Sasse, Brostoff, & Weirich, 2001; Stanton, et al., 2005). Such risks could emerge from careless, unaware, or ignorant handling of new ICT. Current examples are insufficient protection measures or the improvident disclosure of private information.

Thus, harm prevention could benefit from insights into why people may be unwilling to use ubiquitous ICT in the intended way, and why they might not undertake certain protective behaviors.

4. Objective of the thesis and overview of the research questions

The overall objective of this thesis was to gain a better understanding of the relevance of individual behavior with respect to susceptibility, mitigation, and production of the risks of ubiquitous ICT. Better insights into the human factor in relation to these risks are considered to be a precondition for the identification of attachment points for policies lowering risks in the development and use of ubiquitous ICT.

This section gives an overview of the aims and research questions regarding the overall contents of the thesis. Further aims which emerged from the specific context of the individual studies are included within the corresponding chapters, and methodological requirements that emerged from the procedure are specified in the subsequent section 6 in this chapter.

A first objective was to find out how risks of ubiquitous ICT are appraised by potentially concerned people, i.e., ordinary citizens. To this end, the following research questions were posed:

a) What changes do individuals expect from ubiquitous ICT?
b) What trains of thought lead people to arrive at their expectations? Thus, what are the attributed drivers of the expected changes?
c) Which components impact people's appraisal of the threats of ubiquitous ICT?

The second aim of this thesis was to increase knowledge regarding the preconditions of protective behaviors. Ideally, individuals will use ubiquitous ICT in a competent and self-determined way, and are free to decide on the degree and quality of their technological involvement. This includes precaution and competent coping with the risks of ubiquitous ICT. Understanding the preconditions of individual protective behaviors is a premise for the support of competent coping with the adverse effects of ubiquitous ICT. The aim was to improve this understanding by answering the following research questions:

d) What protective behaviors do people consider useful against the risks of ubiquitous ICT?
e) What components impact people's appraisal of coping efficacy in dealing with threats from ubiquitous ICT?
f) To what extent do the perceived threat and coping efficacy predict the intentions to take protective actions against these threats?
g) How does negative affect influence behavior choice?
h) How will the level of an individual's protective behaviors evolve over time, under changing external impacts?

A third aim was the closer examination of potential individual causes of risks of ubiquitous ICT. Of interest in this respect was the emergence of reactance, as well as the preconditions for the omission of protective behaviors:

i) What potential reactance may emerge from the perception of the risks of ubiquitous ICT?
j) To what extent do perceived threat and coping efficacy predict undesirable responses, such as technological overstrain, helplessness, and denial?
k) How will the level of an individual's non-protective reactions evolve over time, under changing external impacts?

5. Context of the thesis

This thesis was embedded in a project of a research cooperation entitled 'Cooperative Assessment and Communication of Systemic Risks of Ubiquitous Information and Communication Technologies (AACCrisk)' (www.aaccrisk.de), which was part of the thematic topic 'Strategies for Coping with Systemic Risks' of the research program 'Social-Ecological Research (SÖF)' of the German Federal Ministry of Education and Research (BMBF). Partners of the research cooperation were the 'Institute for Social-Ecological Research and Education (Ecolog)' in Hannover, 'Sinus Sociovision' in Heidelberg, and the 'Interdisciplinary Center for General Ecology (IKAOE)' at the University of Bern (the host of the author of this thesis). The research cooperation encompassed three subprojects: Within the first subproject, potential ubiquitous ICT settings were described and their risks were assessed from experts' viewpoints (Behrendt, et al., 2007; Neitzke, et al., 2006; Neitzke, et al., 2008). The work described in this thesis was part of the second subproject, which investigated the perception of and potential reactions to the risks of ubiquitous ICT in the population (Forschungsverbund AACCrisk, 2008; Wippermann, 2007). Within the third subproject, recommendations on precaution and targeted risk communication were developed (Kleinhückelkotten & Neitzke, 2009; Neitzke & Vedder, 2010).

6. General procedure and organization of the thesis

The above-listed aims and research questions of this thesis were addressed by means of an iterative procedure which alternated between theoretical consolidation and three conceptual as well as empirical studies. The procedure is outlined in Figure 1.1. This illustration further assigns the research questions presented above to the individual studies.

Step 1: As denoted in Figure 1.1, in a first step, the theoretical background had to be acquired regarding individual mental representations of risks, a qualitative elicitation method had to be chosen, and the general topic 'risks of ubiquitous ICT' had to be narrowed down and specified. The mental model approach (Böhm & Pfister, 2001; Morgan, Fischhoff, Bostrom, & Atman, 2002) was selected as a theoretical basis, which will be detailed in section 7.1 of this chapter, and section 3 of chapter 2. To collect data, the 'Cognitive Mapping'[1] method was adapted. In section 4.1 of chapter 2, this method is presented more specifically. Based on scenarios described in the first subproject of the research cooperation (Neitzke, et al., 2006), the decision was taken to restrict this first study to applications of ubiquitous ICT in the health sector. In contrast to the areas of living, consumption, work or individual traffic, the ICT developments in the health sector will concern the most people and their technological implementation may lie outside the boundaries of individual discretion.

Step 2: In a second step, qualitative interviews were conducted and analyzed based on the 'Cognitive Mapping' method. Thereby, key concepts and mental structures regarding risks of ubiquitous ICT were identified. The detailed description of this first study can be found in chapter 2.

Step 3: The results of the first qualitative study revealed the insight that a better understanding of the emergence of protective behaviors regarding the risks of ubiquitous ICT and their omission is needed (cf. objectives 2 and 3 in section 4). With this in mind, and depending on the key concepts identified in study 1, the next step (3a) encompassed the search for a theoretical framework explaining the premises of protective and non-protective behavior. This was found in the form of the protection motivation theory (Rogers, 1975, 1983), (cf. 6.2 in this chapter and 2 in chapter 3), which was supplemented with further psychological risk concepts. Following these theories, a model of the relationships between characteristics of subjective threat appraisal components and protective as well as non-protective reaction intentions was hypothe-

[1] The method 'cognitive mapping' has nothing to do with 'cognitive maps' (e.g. Kitchin, 1994), which reproduce spatial representations of geographical locations.

sized. To test this model, items were formulated on the basis of the results from study 1 (step 3b).

Step 4: Under the lead management of our research cooperation partners 'Sinus Sociovision', a representative survey was conducted with the help of a standardized questionnaire. The topic of the survey was the use and perception of current ICT and prospective ubiquitous ICT. Thus, the potential applications of ubiquitous ICT were covered in a broad and general way. Data collection, data analysis, and the results of this second study are described in chapter 3.

Step 5: The results of the quantitative survey highlighted the relationships between individual risk perception and behavior intention. However, it was realized that the model used only reflected limited extracts of the whole appraisal process. In particular, it failed to attend to the dynamic and reciprocal characteristics of the appraisal process over time. This evoked the need to resolve the unidirectional, linear relationships, and to create a model describing the relationships between individual risk perception and protective behavior reciprocally and dynamically.
Thus, within step 5, the groundwork for the conceptualization of a dynamic model was prepared: the discussion of the shortcomings of study 2 (cf. section 6.1 in chapter 3) stimulated a theoretical examination (step 5c) of control-theoretical frameworks on self-regulating behavior (Liang & Xue, 2009; Powers, 1973; Wilde, 1982b; described in more detail in section 6.3 in this chapter, and in section 2 in chapter 4). Study 2 provided structural elements (step 5b), and study 1 increased the general understanding of the basic subjective system structures (step 5a).

Step 6: The sixth step encompassed the conceptualization and testing of the theory-based, mathematical model of individual threat control, which allowed for the simulation of behavioral progressions over time. The model conception and formalization was accomplished according to system dynamics methodology (Forrester, 1961; Sterman, 2000). The model derivation and testing is detailed in study 3 in chapter 4. The model was restricted to the explanation of security behavior with respect to existing ICT applications. In doing so, the work was able to benefit from existing theories and empirical research on concrete, observable information system security behavior. Hence, the model was developed in a more concrete and consistent way. The relevance of the model regarding ubiquitous ICT will be an issue in the overall discussion in chapter 5 (section 2).
This was the final step carried out within the present thesis. However, the research procedure cannot be considered to be concluded. Implications for further research (and practice) are one of the topics of the overall discussion in chapter 5 (cf. section 4).

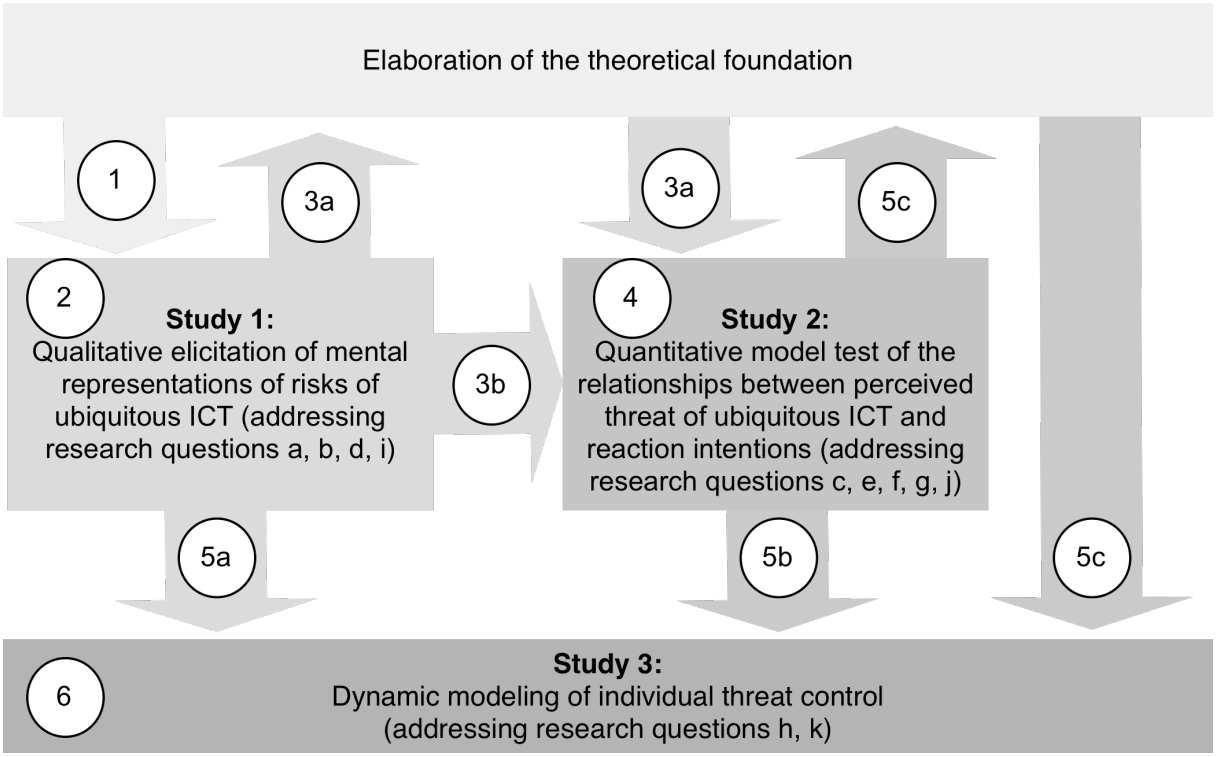


Figure 1.1. Organization and operational research steps (enumerated in circles) of the procedure of the thesis.

7. Psychological theoretical frameworks on risk appraisal and the building of protective or non-protective reactions

In order to attend to the different human aspects of individual risk perception, production, and mitigation, different theoretical approaches have been considered. This paragraph gives an overview of the risk theoretical frameworks relevant to this thesis. Besides general risk-psychological theories, the main theoretical focus relied on environmental psychological applications, since the risks of ubiquitous ICT settings showed parallels to (natural) environmental risks. The theoretical foundation was supplemented with health-psychological approaches and applications used to explain security behavior in relation to traffic and IT risks.

The different theoretical frameworks were deployed in different parts of the thesis, as explained in section 6: A first theoretical thread encompassed the individual mental representation of risks. The mental models approach, upon which study 1 (chapter 2) was based, will be presented below. A second thread concentrated on the prediction of behavioral reactions to appraised risks. These theories were mainly used in study 2 (chapter 3). And a third, lesser known, theoretical thread defined the perception vs. behavior relationship as a reciprocal process, i.e., high- and low-risk behavior is understood as cause and consequence of risk perception. These so-called cybernetic or control theories were the basis for study 3 (chapter 4).

7.1. Subjective, mental representations of risks

Laypersons' risk judgments are no simple harm x expectancy calculations. Rather, they are based on multifaceted, individual, subjective mental representations of risk. Two different traditions of risk representations exist (Böhm, 2008). One approach, the psychometric paradigm, examines the importance of different dimensional aspects for the risk judgment of individuals (Slovic, 1987, 1992; Slovic, et al., 1982). This approach will not be detailed further since it only played a minor role in this thesis.

The second approach examines risk representations in the form of mental risk models. So far, no consistent definition exists of how mental models are understood in psychology (Doyle & Ford, 1998). For this thesis, mental models were considered to be individual, internal naïve theories (Opwis, 1985) or knowledge representations (Doyle & Ford, 1998; Gentner & Stevens, 1983; Thüring & Jungermann, 1986) about the elements and structure of an external system. Mental models are built by integrating new experiences and knowledge about the target system within existing representations (Norman, 1983).

The mental model approach has its origins in cognitive psychology (Gentner & Stevens, 1983; Johnson-Laird, 1983; Newell & Simon, 1972; Rouse & Morris, 1986), but has increasingly been applied in risk research. Mental risk models encompass notions about causes and consequences of risks (Böhm, 2008). The approach has been used to identify laypersons' knowledge gaps and faulty conceptions of the emergence of risks (as used for example by Bostrom, Morgan, Fischhoff, & Read, 1994; Read, Bostrom, Morgan, Fischhoff, & Smuts, 1994) in order to design targeted risk communication (Bostrom & Fischhoff, 2001; Morgan, et al., 2002). Other authors have developed risk classifications from the examination of mental risk models (Böhm, 2003; Böhm & Pfister, 2000). Moreover, it is also assumed that people mentally simulate system constellations, as well as behavior alternatives, on the basis of mental models in order to make prognoses and anticipations about the future (Rouse & Morris, 1986; Thüring & Jungermann, 1986).

The mental model approach, however, is limited in the sense that mental models are about mental contents, and their associative relations (Doyle & Ford, 1998; Rouse & Morris, 1986). Information about mental processes or underlying structures must be concluded indirectly or examined with other approaches. Therefore, the next selection of theories used in this thesis was about cognitive risk appraisal processes and their impact on risk-relevant behavior.

7.2. Theoretical frameworks predicting protective and non-protective behaviors on the perceived risk

Whereas the mental risk representation theories presented above encompass different aspects of risk appraisal, the theories presented in this paragraph go one step further. They relate individual risk or threat appraisal to potential protective reactions, such as attitude changes, the forming of behavioral intentions, or behavior changes. This is due to understanding perceived threat as a predictor of a reaction at a single point in time.

Probably the most prominent theoretical approach in this regard is the protection motivation theory (PMT) of Rogers (Rogers, 1975, 1983; Rogers & Prentice-Dunn, 1997)[2]. This theory assumes risk information to be mediated by two appraisal processes before it impacts behavior. In the first mediating process, the threat appraisal process, the danger is evaluated in terms of its severity and probability to do harm. The second appraisal process evaluates options for coping with the danger, with respect to perceived self-efficacy, response efficacy, and costs of the mitigating behavior. The probability of a protective behavior increases under high perceived threat and coping efficacy, whereas high perceived threat and low perceived coping efficacy result in so-called non-protective reactions, such as the denial of the threat.

PMT stands in the tradition of fear appeal theories (Eagly & Chaiken, 1993; Witte & Allen, 2000). Earlier theories on the impact of fear appeals interpreted fear, i.e., emotional arousal, as the main cause of behavioral reactions (Hovland, Janis, & Kelley, 1953; Janis, 1967; McGuire, 1969). Following the spirit of the age, Leventhal (1970) was the first researcher to describe, with his parallel response model, a cognitive process (danger control) accompanying fear control. PMT adopted the danger control process by integrating an expected value approach (severity x probability). Furthermore, PMT enclosed constructs of Lazarus' stress theory within the coping appraisal process (Lazarus, 1966).

PMT has found most application and empirical support in health psychology (for a meta-analysis see Floyd & Prentice-Dunn, 2000; Milne, Sheeran, & Orbell, 2000), but has also been adapted for environmental hazards (Gardner & Stern, 1996). Applications of the PMT framework to environmental risks are increasing (e.g., Grothmann & Reusswig, 2006; Homburg & Stolberg, 2006; Martens & Rost, 1998). Recently, the framework has also been used with respect to the risks of information and communication technologies (Kuttschreuter & Gutteling, 2004a, 2004b; Workman, 2007; Workman, Bommer, & Straub, 2008).

In the literature, several limitations of the PMT framework have been identified. For example, PMT has been criticized for neglecting the original main cause 'fear' (Eagly & Chaiken, 1993;

[2] A further framework explaining protective behavior is the Health Belief Model (Janz & Becker, 1984). This model, however, has been criticized for the low specificity of its constructs (Armitage & Conner, 2001). It was not considered further in this thesis.

Witte, 1998). Recent fear appeal theories, such as the extended parallel process model (EPPM) of Witte (1994, 1998), pay more attention to this aspect. Furthermore, PMT ignores potential sequential processes. The most recent approaches try to integrate PMT into stage models (Block & Keller, 1998; Cismaru, Lavack, Hadjistavropoulos, & Dorsch, 2008). Finally, the authors of PMT acknowledge a 'lack of knowledge about how people's long-term coping behaviors feed back into and affect the cognitive mediating processes' (Rogers & Prentice-Dunn, 1997, p. 128).

The lack of integration of feedback processes by unidirectional predictive models, explaining protective behavior, has at least been addressed in conceptual terms by frameworks presented in the subsequent paragraphs.

7.3. Cybernetic frameworks of risk behavior

To the best of my knowledge, there have been two different attempts to explain individual risk behavior with cybernetic frameworks. The first attempt, the Risk Homeostasis Theory (RHT) of Wilde (1982b, 1998), has persisted for several years, whereas the second theory, the Technology Threat Avoiding Theory (TTAT) of Liang and Xue (2009), has been published only recently. Both approaches will be presented below after introducing basic information about cybernetic theories.

Cybernetic theories (Ashby, 1956; Wiener, 1948) emerged from engineering control theories which paid attention to homeostatic, self-regulating mechanical operations (Richardson, 1991). Cybernetic theories transferred principles of the mechanical theories to human behavior. Thus, the cybernetic control theories understood human behavior as embedded in a self-regulating process. Specifically, human control theories tried to explain stability in behavior under changing environmental impacts over time (Richardson, 1991; Vancouver, Putka, & Scherbaum, 2005). The basic unit of control theories is a discrepancy-reducing or goal-seeking feedback loop, which consists of a minimum of three related components. The first is the perceived current environmental state. This perception is compared to the second component: an internal reference value or goal. A possible discrepancy between these two components activates the third element, which is a corrective behavioral reaction aimed at bringing the environmental state in line with the internal goal.

Numerous psychological theories contain, at least implicitly, control-theoretical assumptions (Edwards, 1992). Explicitly, they have been adapted and advanced, for example, by Powers (1973), Carver and Scheier (1982, 1990), Levine (1992), and Vancouver (Vancouver, et al., 2005; Vancouver, Thompson, Tischner, & Putka, 2002; Vancouver, Thompson, & Williams, 2001). However, a mismatch between theoretical and empirical cybernetic works can still be observed (Edwards, 1992).

Over twenty years ago, the homeostatic principles inspired Wilde to formulate the risk homeostasis theory (RHT), also named risk compensation theory (Wilde, 1982b, 1998). This theory posits that individuals compare their perceived level of risk with their internal target level for that risk. In the case of an exceeded target level, risk-mitigating behavior is increased. If the perceived level of risk falls below the target level of risk, protective behavior is reduced. According to the RHT, this may occur when the perceived external danger changes due to, for instance, structural safety measures.

RHT provoked a lively scientific debate (Trimpop, 1996), not least because the theoretical conceptualization of the components, as well the empirical evidence put forward, were seen to be controversial (Evans, 1986; Slovic & Fischhoff, 1982; Thompson, Thompson, & Rivara, 2001), and have not been scientifically resolved to date (Trimpop, 1996).

With the Technology Threat Avoiding Theory, a new control-theoretical framework explaining protective behavior has recently been developed by Liang and Xue (2009), independently of the RHT (at least the authors do not quote the RHT). This approach tries to integrate aspects of Rogers' Protection Motivation Theory (PMT) into a cybernetic structure. However, the authors did not adapt the classical goal-seeking feedback structure, but assumed that risk-avoiding behavior is based on a goal-avoiding loop. The TTAT lacks empirical foundation, and acknowledgement of the scientific debate has yet to appear.

Chapter 2:
Qualitative Exploration of the Public Representation of Ubiquitous ICT Applications in the Outpatient Health Sector

This chapter is an early version of an article published as:
Moser, S., Bruppacher, S.E., & DeSimoni, F. (in press). Public Representation of Ubiquitous ICT Applications in the Outpatient Health Sector. *International Journal of Technology and Human Interaction.*

Abstract

Current technological developments in the field of information and communication technologies (ICT) are bringing about a new generation of ICT applications: New ICT devices are smaller, more powerful, and better integrated into everyday devices and objects, opening up new possibilities, especially for health monitoring. To date, scientific interest has mainly been limited to current ICT applications, ignoring new trends and their social impact. The present study makes a first attempt in this direction by investigating public representation of future ICT applications in the outpatient health sector in terms of their social acceptance, expected changes on the individual and societal levels, and the health-related behavioral change potential. Mental models of future ICT applications were elicited from eleven interviewees with the help of a qualitative, visual interview technique. The findings revealed that the interviewees felt ambivalent about anticipated changes; only if ICT use were to be voluntary and restricted to single applications and trustworthy institutions did interviewees expect individual benefits. Concerns about data transmission to unauthorized third parties, and widespread technological dissemination forcing compulsory participation led people to feel averse to such technology, which, in turn, may undermine its technological effectiveness. In this case, individuals seemed unwilling to consider new ICT applications. Implications of the findings for potential implementation of future ICT applications in the outpatient health sector are discussed.

Keywords: Ubiquitous Information and Communication Technologies, Health, Behavior Change, Mental Models, Ubiquitous Computing, Pervasive Computing

1. Introduction

Over the last few decades, advances in information and communication technologies (ICT) have been changing many aspects of modern society, including the health sector. New ICT applications, mostly subsumed under the term 'e-health', have facilitated access to and exchange of health-related information by different partners of the health sector. The diffusion of ICT into the health sector has led to, for example, changing operation processes, new forms of patient information-seeking behaviors, and changes in physician-patient relationships (Andreassen, Trondsen, Kummervold, Gammon, & Hjortdahl, 2006; Kivits, 2006; Tautz, 2002). These changes have attracted growing scientific interest; since the turn of the millennium, the number of publications related to e-health has increased markedly (Ahern, 2007; Curry, 2007).

However, most of this research has concentrated on current ICT applications mainly based on the Internet. Only rarely has attention been paid to present and prospective technological changes in the direction of increased interconnected, omnipresent and embedded ICT applications, as well as to the social impacts that might accompany these changes. Current and prospective technological possibilities may increasingly become ubiquitous in daily life in general, and in particular pervade the health sector. The purpose of this study is to address the potential long-term impacts of ubiquitous ICT in the outpatient health sector from a user perspective. The aim was to explore individual expectations and acceptance of the diffusion of ubiquitous ICT applications, and their potential to support healthy behaviors. In so doing, the following questions were addressed:

- What changes do individuals expect from ubiquitous ICT?
- What trains of thought lead people to their expectations? Thus, what are the attributed drivers of the expected changes?
- What potential for supporting users' health-related behavior do ubiquitous ICT applications offer? What potential reactance may emerge?
- And what protective behaviors do people consider useful against the risks of ubiquitous ICT?

Before turning to the research approach and the investigation, the next section presents the ongoing and expected technological trends in the outpatient health sector.

2. General technology trends and potential impacts in the outpatient health sector

Accelerating advances in ICT are often explained by Moore's Law, which states that the power of microprocessors roughly doubles every eighteen months (G. E. Moore, 2003). The consequence of this continuing exponential growth is that microchips and storage components have and will become increasingly more powerful, smaller, and cheaper (Mattern, 2005), allowing them to be embedded in everyday objects such as furniture, household appliances and clothing. Through Internet, radio transmitters, infrared, or Bluetooth, such 'smart objects' can be identified, localized and linked to associated data records and broader sensor networks. They are thereby enabled to interactively explore their environment (e.g., collect and deliver environmental data such as temperature, location and speed) and to respond to other smart things or human beings. This vision of invisible, smart computers assisting individuals' everyday tasks almost anywhere and at any time, has been called 'ubiquitous computing' (Weiser, 1991).

The technological advances of ubiquitous ICT have not remained hidden to trendsetters in the health sector. Potential applications range from smart consumer-goods packaging that might allow for diet monitoring, to clothes that might attend to physical training by recording bodily indicators, such as the duration and intensity, to portable devices that register bodily indicators, such as blood pressure, glucose level and substance use. Sensor networks may allow for these registered indicators to be automatically transmitted to a patient's electronic health record, with the option to generate warning signals to the patient (or directly to the corresponding medical service) if there is significant deviation from normal values. As a feature of 'smart homes', such ubiquitous ICT applications may compensate for handicaps and support convalescence or aging on site (S. Brown, et al., 2004; Dengler, Awad, & Dessler, 2007; IAF, 2006; The Royal Society, 2006).

Expected benefits from ubiquitous ICT applications in the outpatient health sector may be increased convenience and autonomy for those in need of care, as well as health cost reductions and increased efficiencies in health administration and health care (S. Brown, et al., 2004; Tan, 2005; Tautz, 2002). Furthermore, ubiquitous ICT applications are assumed to include several features which may enhance individual preventive health behavior; they are accessible independently of time and location, and allow for a widespread dissemination of general information as well as for tailored and personalized information, feedback and interactivity (Curry, 2007; Evers, Prochaska, Driskell, Cummins, & Velicer, 2003; Fogg, 2003; Neuhauser & Kreps, 2003). Since a considerable portion of healthcare costs is caused by modifiable risk factors such as smoking, alcohol or substance use, lack of physical activity, or unhealthy nutrition (McGinnis, 2001), there is a growing interest in the preventive application of ubiquitous ICT in the outpatient health sector in order to support and monitor health-related behavioral changes.

However, in order to establish efficient ubiquitous ICT services in the outpatient health sector, public acceptance is needed. First of all, general public agreement is needed in order to set up, convert and interconnect the health services on an electronic basis. And secondly, users have to be able and willing to apply the technology in the intended way. Public opposition could defer, or even prevent, ubiquitous ICT implementation, and incomplete or inaccurate use may obviate its potentials, or even create yet unknown risks (The Royal Society, 2006).

3. Exploring individuals' anticipations with mental models

In order to shed light on people's anticipations about possible long-term developments, such as the diffusion of ubiquitous ICT applications in the health sector, the elicitation of mental models seems particularly suitable. The mental models approach has a tradition in cognitive (Gentner & Stevens, 1983; Newell & Simon, 1972) and risk psychology (Morgan, et al., 2002). Mental models can be defined as individually held naïve theories (Opwis, 1985) or knowledge representations (Doyle & Ford, 1998; Gentner & Stevens, 1983; Thüring & Jungermann, 1986) about the functioning of human interactions with or within complex systems. Examples of such empirically investigated systems are technological devices (e.g. pocket calculators in Young, 1983), ecological systems (e.g. global climatic change in Bostrom, et al., 1994; Read, et al., 1994) or social systems (e.g. teams in Langan-Fox, Code, & Langfield-Smith, 2000). Mental models are formulated and modified through interactions with the target system (Norman, 1983). They are assumed to be found on associative networks in the memory (Langan-Fox, et al., 2000), and to contain an individual's subjective assumptions about the causes and consequences of system changes in order to reason (Johnson-Laird, 2006), i.e., to make sense of the world.

Crucial to this investigation is the assumption that people explore the future on the basis of an underlying mental model (Rouse & Morris, 1986; Thüring & Jungermann, 1986). Thus, people let their mental model 'run' in their mind's eye if asked for a prognosis or decision, in order to anticipate the potential outcome of a certain situational constellation of their own or others' behaviors. As Böhm and Pfister argue, mental models are 'the fundamental cognitive structures on which risk perceptions ... and behavioral decisions are based' (Böhm & Pfister, 2001, p. 23). These authors demonstrated that differences in the causal structures of mental models were related to different responses, such as help, aggression, escape, political action, and self-focus (Böhm & Pfister, 2000). Thus, people consider different action alternatives, depending on the consequences they anticipate on the basis of their mental models. The investigation of these models therefore allows not only the elucidation of the causally linked knowledge structure concerning a certain scenario, but also the response tendencies they evoke.

4. Method

4.1. Methodological approach

In view of the innovative nature of this research topic, an exploratory qualitative approach seemed appropriate, since only an open-ended method guaranteed a broad identification of contents and structures of mental models which people hold about ubiquitous ICT applications in the outpatient health sector. Therefore, an approach termed 'Cognitive Mapping' (Bryson, Ackermann, Eden, & Finn, 2004; Eden, 1992) was adopted. This method is based on Kelly's theory of personal constructs (Kelly, 1955), from which also the better known repertory grid method originates (Bannister & Fransella, 1980). The cognitive mapping method was originally used in operational research (Eden & Ackermann, 2004). It is designed to create visual 2-D representations of ideographic patterns of causally linked concepts. 'Concepts' are understood in a broader sense, containing not only 'knowledge units', but also constructs such as 'goals', 'values' or 'action intentions'. Concepts are represented by nodes, which contain a concept's description in note form, and are linked by arrows, which stand for positive or negative causal relationships between the corresponding concepts. To elicit an individual 'map', the 'laddering' technique (Hinkle, 1965, cited in Bannister & Fransella, 1980) is used: Interviewees are asked 'why' they mentioned a certain concept, i.e., what the concept's implications are ('laddering' up to elicit the consequences), and 'how' the concept is achieved, i.e., what the concept's reasons are ('laddering' down to elicit its causes). For applications of the 'laddering' technique, see e.g., Taylor, Bagozzi, Gaither and Jamerson (2006).

The visual support of 'cognitive mapping' helps to structure, organize, and analyze complex, systemic data (Eden & Ackermann, 2004). Its implementation is facilitated by the computer software Decision Explorer®, which was specifically designed to elicit and analyze 'cognitive maps'. A further advantage of this technique is its constructivist approach; whereas in most other mental-model approaches, concepts are given to the interviewees, and/or their relations retrospectively identified by the researcher, 'cognitive mapping' is done by elaborating content and structure during the interview session, in cooperation with the interviewee (for an overview of elicitation and representation techniques of mental models, see Langan-Fox, et al., 2000).

4.2. Procedure

The interviews were conducted by the first author in October 2006 in Berlin, Germany. They were held in the interviewees' home or workplace and varied in length between one and four hours. All of them were tape-recorded with the interviewees' informed consent.

The interviews started with demographic questions and questions about their current use of ICT. Next, the cognitive-mapping method was introduced to the interviewees by demonstration with a short example how causal structures can be displayed in the desired visual form of nodes and arrows. After this, the interviewees were introduced to the topic of ubiquitous ICT in the outpatient health sector with the help of a leaflet (see Figure 2.1). This leaflet described different ubiquitous ICT applications, imitating a health insurer's advertising brochure. Interviewees were informed that the leaflet was formulated by the researcher, i.e., it was fictitious, but that the technologies mentioned are already available or in preparation. Interviewees were asked to imagine living ten to fifteen years in the future, receiving this leaflet from their health insurer.

The individual maps were created on a laptop with the Decision Explorer® software directly during the interview, involving the interviewee in this task. Following the procedure recommended by Morgan et al. (2002), the interview was started with an open question by asking the interviewee if he or she could imagine participating in the health program offered. After responding to the opening question, the interviewees were invited to comment on their decisions by explaining what they believed their participation would change. Most interviewees described their thoughts in a narrative way. Their representation in the form of nodes and arrows was then jointly developed by the interviewee and the interviewer through discussion. The emerging chains of anticipated consequences were laddered up until reaching the level of general (anti)goals, such as 'totalitarian system', or 'healthier population'. If interviewees had already answered the entry question on this general level, they were asked to explain exactly how participation in the insurer's program would lead to this general concept. This procedure was continued until the interviewee stated that no further consequences could be drawn. Then, interviewees were asked to explain situations or conditions under which they could imagine participation or no participation (thus laddering down). All individual maps, which emerged during the interview sessions, are depicted in Appendix A.

After completing the full interview, the interviewees received €20 in appreciation of their participation.

4.3. Interviewees

Interviewees were recruited using a snowball technique; starting with persons from the authors' circle of acquaintances, who, in turn, suggested further interview partners of interest. Recruitment was stopped after eleven interviews. Three female and eight male interviewees took part (see Table 2-1). Their age ranged from 26 to 42 years, with a mean of 32.2 years. Three of them were students, one employed at the university, one employed as a waiter, and six were self-employed in a range of professions (self-employment having become increasingly common in Germany). Two had acquired professional IT skills, as they worked regularly or part-times as IT

consultants. None of the interviewees had specific experience with ICT applications in the health sector; however, all mentioned using current ICTs such as the Internet.

Table 2-1: Interviewees' details

Interviewee	*Age*	*Profession*	*Previous use of Internet / ICT applications*
'Anne'	28	Student	Information, e-mail, chatting, shopping
'Anthony'	28	Self-employed IT-supporter	Information, communication, downloading of updates
'Cindy'	30	Student	Information, e-mail, Internet telephoning
'Marc'	41	Self-employed photographer	Information, e-mail, shopping, providing a website
'Eric'	42	Researcher, IT-supporter	Information, communication
'Ben'	26	Student	Information, e-mail, shopping, downloading music
'Michel'	35	Self-employed (no specific declaration)	Information, e-mail
'Helen'	30	Self-employed project manager	Information, e-mail, chatting, Internet telephoning, downloading, learning languages
'Neal'	26	Self-employed author	Information, e-mail, shopping, downloading of updates and movies
'Bob'	40	Self-employed event manager	Information, e-mail (providing a newsletter), 'Skype'
'Donald'	29	Steward	E-mail, Internet telephoning, playing games, reading newspapers

Notes: To protect interviewees' anonymity, names have been changed. The individual maps of all interviewees are depicted in Appendix A.

4.4. Material

In order to help the interviewees understand the topic, a leaflet was created about a health program offered by a fictitious health insurance company (shown in Figure 2.1).

The applications of ubiquitous ICT offered in the leaflet were taken from Neitzke et al. (2006). These authors formulated various scenarios about how ubiquitous ICT might pervade daily life. One of these scenarios addressed the outpatient health sector. The technologies described in the leaflet were derived from current developmental trends, although giving the interviewees the chance to base their reactions on existing technologies was stressed. Thus, some of the applications described do not correspond to the latest developments. The situation of a health insurer as supplier was chosen in order to account for the fact, that within the health sector, ICT applica-

tions have been and will be mainly driven by for-profit companies (Eng, 2004; Fogg, 2003; Neuhauser & Kreps, 2003). Health insurers may have a particular interest in implementing ubiquitous ICT applications in order to reduce the information gap about their customers on their side (Coroama & Höckl, 2004). Pretests revealed that the original form of the input material – a narrative description of the above-mentioned scenario – evoked feelings of unreality and low involvement among the interviewees. Therefore the same content was made to look like a company leaflet, thus attaining greater credibility.

4.5. Data analysis

The data analysis, conducted with the help of the Decision Explorer® software, was carried out in four steps:

Step One: Merging the Individual Maps. In a first step the individual maps were merged into a comprehensive 'cause map'. 'Merging' is an iterative process in which concepts within and between the individual maps are compared and put together, retaining the original causal links (Eden & Ackermann, 1998). The decision to merge two concepts depended on their content (i.e., similar contents were merged into a new unipolar concept, and differing contents into a new bipolar one) and structural position (i.e., similarity of causes and consequences). The merging process yielded an aggregated, condensed 'cause map' that contained all eleven individual maps.

Step Two: Identification of Key Concepts. Second, the cause map was examined for clusters, i.e., groups of concepts on the same topic. From each cluster, the most central, i.e., the most densely linked, concept was extracted as the key concept. Decision Explorer® offers a centrality calculation (Eden & Ackermann, 1992) to determine the number of direct and indirect links of each concept, as well as their weighting according to their level (e.g., direct links were weighted with 1 and indirect links of the first level with .5). This calculation revealed high centrality scores for most of the key concepts identified. However, high centrality scores are impacted by merging, i.e., more frequent merged concepts combined more links from the individual maps and thus reached higher centrality scores. Since we were interested in a qualitative overview per se, and not in representative statements, we also accepted key concepts with lower centrality scores, but which represented an otherwise uncovered topic.

Your health is important to us

We would like to help you both to stay healthy and also to save premiums!

Recent information and communication technologies now allow for an individual health monitoring.

Find out about our health program and let us prepare your individual support package for you.

It takes little effort to lead a good healthy life. The key is a balance of proper nutrition and physical training. Create your own health program by choosing from our offers listed below:

	Functioning:*	**Our standard offer**	**Options**
Physical training condition	Carry our 'sports wear'. Integrated movement sensors collect data about your physical training condition and transmit them to us.	You will be given weekly feedback as to whether you've achieved your quota or how much is missing. Depending on your cooperation and success you will benefit from up to 15% premium discount!**	
Healthy nutrition	Put all your meals on the scale (even snacks!), and enter their composition into the mini computer.	We will evaluate your nutrition on a daily basis, and provide you with recommendations in the form of - recipes - menu advice Depending on your cooperation and success, you will benefit from up to 15% premium discount!**	On our website you can arrange for and order healthy recipes. The required ingredients or the complete meal is delivered to your home by our associated shops. To make manual weighing obsolete, we suggest choosing the complete menus delivered with an RFID label that can be recognized by the mini scale.
Monitoring of bodily indicators	Carry our multitask implant to monitor your pulse, blood sugar, and cholesterol level 24/7. A multitask watch informs you immediately about possible changes.	Implantation is free; we monitor your bodily indicators 24/7, and inform you immediately if a critical threshold is exceeded.	Possibility of direct transmission of critical indicators to your family doctor, so that he can attend to you immediately.
Avoidance of unhealthy lifestyles	As has been proven, smoking and excessive consumption of alcohol harms your health. Carry our implanted detectors, which alert you in the case of over-consumption via a multitask watch.	Implantation is free.	

* All data are transmitted from the sensors, via local radio network, to your mobile phone, and from there automatically to our central office.
** Our computerized monitoring program registers the discounts automatically with your account.

Figure 2.1. Input material for the interviews: Fictitious leaflet of a health insurer offering its clients a technology-supported health monitoring.

Notes: Above: front side, below: inside. Version translated from German to English.

Step Three: Classification of Key Concepts. Next, according to their content, the key concepts identified were classified as 'consequences', 'causes', or 'actions'.

Step Four: Comprehension of the Linking Structure between the Key Concepts. Finally, to understand the context of the key concepts, the linking chains between the key concepts were detailed with the help of the cause map. The outcomes of this final step of analysis are different simplified representations of the cause map containing the key concepts of interest, as well as their structural interconnectedness.

5. Results

In the following section we provide insights into the key concepts identified, as well as in their structural interconnections. This is done with help of a series of five simplified visual representations. First, Representation A in Figure 2.2 shows the shared aggregated basic structure of identified key consequences that resulted from the merging procedure. Next, the example of the key consequence 'loss of versus gain in control' is detailed (Representation B in Figure 2.3). Then, the structural embedding of the actions 'participation in the insurer's health program' (Representation C in Figure 2.5), 'change or refusal to change health-related behavior' (Representation D in Figure 2.6), 'to search for information', and 'to protest' (Representation E in Figure 2.7) is described.

5.1. Basic belief structure of expected consequences of ubiquitous ICT applications in the outpatient health sector

Key concepts categorized as 'consequences' can be arranged, as is shown in Figure 2.2, with the help of two identified key 'causes' (in arrows): the 'general acceptance and dissemination of ubiquitous ICT' in society and the 'data transmission' of sensitive data from a health insurer to third parties. Depending on whether the interviewees supposed these two developments would occur, all expected key consequences could be allocated to one of four groups (shown in the 4-quadrant table in Figure 2.2). The groups differed first as to whether the consequences would affect the individual user only, or, in the case of widespread dissemination of ubiquitous ICT, all of society, i.e., non-users also. Second, the expected consequences varied as to whether the interviewees assumed the data-exchange to be restricted to the user and the health insurer or whether they suspected the data would be transmitted to further actors, such as the government, private industry or other individuals, due to data hacking or selling, or security deficiencies in the storage or transmission of data.

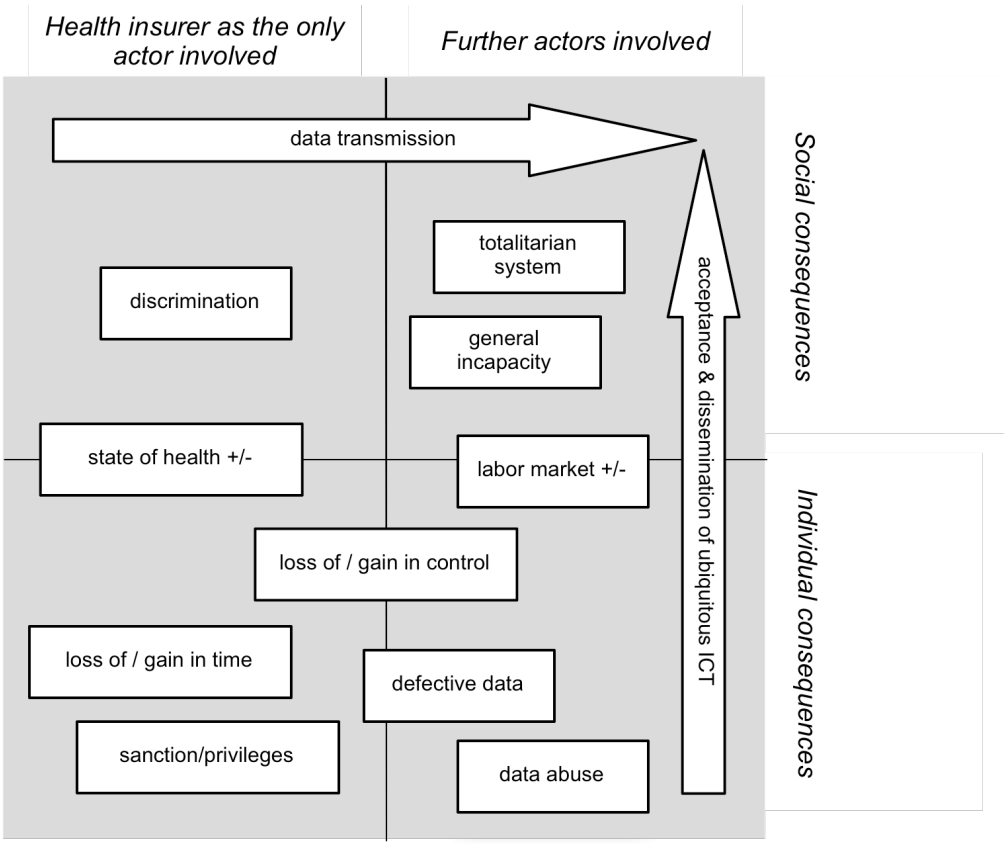


Figure 2.2. Representation A: Basic belief structure of expected consequences of ubiquitous ICT applications in the outpatient health sector.

Note: Key consequences (in rectangles), arranged according to two key causes (in arrows).

Anticipated immediate consequences for individual users interacting exclusively with the health insurer as the only actor with access to the data (shown in the lower left quadrant in Figure 2.2), can be characterized by ambivalence. Interviewees anticipated losses of as well as gains in time and control, positive as well as negative impacts on their own state of health, and sanctions as well as privileges (e.g., premium discounts or increases, shorter or longer queuing time for health services, refusal of cost absorption).

Conversely, anticipated long-term consequences were judged to be negative, with the exception of the ambivalent impacts on the labor market. Increased interconnectedness of data files, due to data transmission, was seen to be accompanied by increased defective and abusive incidents (in the lower right quadrant in Figure 2.2). Increased diffusion of ubiquitous ICT in different life domains was perceived to provoke discrimination of people who are unwilling or unable to follow this technological trend (as shown in the upper left quadrant in Figure 2.2). Finally, as shown in the upper right quadrant in Figure 2.2, under the assumption that both developments - technology dissemination as well as transmission of data – would occur, interviewees anticipated highly undesirable social changes, such as people's increased 'general incapacity' and the emergence of a 'totalitarian system'.

5.2. Loss of versus gain in control

Of the key consequences identified, the concept 'loss of versus gain in control' attained the highest centrality score and will therefore be detailed in the following. Its merged original statements are listed in Table 2-2. Concerning the loss of control, the statements ranged from rather general ones, such as 'heteronomy / intrusion into own life' (Anne) or 'intrusion into personality' (Helen), to very specific assertions resulting from the use of ICT, such as 'restrictions of freedom to choose what to eat or drink' (Donald), or '… when to consult a doctor' (Neal). Conversely, interviewees also expected a certain gain in control due to the use of ubiquitous ICT, e.g., an 'increase in personal freedom' (Marc), or a 'gain in control over otherwise unobservable indicators' (Eric).

Table 2-2: Merged original statements of the concept 'loss of versus gain in control'.

Interviewee	***Statements (translated from German to English)***
'Anne'	'Loss of self-determination / not to be the boss of one's own body anymore (e.g., how many glasses of wine to drink)' 'Food restrictions (no freedom of choice)' 'Heteronomy / intrusion into own life' 'One's own control of a healthy lifestyle is not possible anymore'
'Anthony'	'Decrease in personal freedom'
'Cindy'	'Responsibilities / decisions are relegated to the health insurer' 'Self-control is lost / is taken over by the health insurer'
'Marc'	'Increase in personal freedom'
'Eric'	'The health insurer automatically intervenes when he thinks that I need something, instead of me seeking contact when I want' 'Loss of control over different domains of one's own life (taken over by the health insurer)' 'Gain in control over otherwise unobservable (bodily) indicators' 'Few people understand the system / are able to control the system'
'Ben'	'Otherwise unobservable data become perceptible' 'Own control of the data'
'Michel'	'Disposal / avoidance of responsibility'
'Helen'	'Loss of freedom of choice (restricted supply)' 'Intrusion into personality' 'Responsibilities are taken over by the health insurer (expansion of its competences)' 'Loss of personal responsibility over one's state of health'
'Neal'	'Unnecessary services are imposed (e.g., the family doctor automatically intervenes)' 'Health insurer exerts control' 'Unobservable / perceptible indicators become controllable (e.g., heart attack)' 'No self-control over one's own health / no freedom of choice (e.g., when to consult a doctor)'
'Bob'	-
'Donald'	'Restriction of freedom to choose what to eat or drink' 'Feeling controlled'

The embedding of the key concept 'loss of versus gain in control' into the basic structure is illustrated in Representation B (in Figure 2.3): Attributed causes (shown by in-pointing arrows) were threefold: The first was 'insurer's data analysis and feedback'. Interviewees argued that the insurer's data analysis and feedback would make people lose the ability to recognize and interpret their body's signals, or that laziness would make people delegate the responsibility over their own body to these technologies. Interviewees feared that applying ubiquitous ICT would provoke a loss of coenaesthesia, as well as an inability to survive without technological support, and that technological dependence would be increased by the fact that complex technologies were non-transparent for most users. However, Ben, Eric, and Neal also believed that the feedback provided would allow for positive effects, such as an early diagnosis or prevention of serious diseases. External data analysis and feedback were thus regarded as both desirable and undesirable.

Interviewees saw 'data transmission' as a second cause of loss of control, which would facilitate data abuse. Anthony and Helen suspected they would be swamped by personalized spam. Eric feared a reversal of the burden of proof, i.e., that suspected persons would have to prove their innocence rather than a court of law having to prove their guilt. Eric, Ben, and Helen believed that innocent people would be prosecuted if their data profile unfortunately resembled that of a suspect. Furthermore, Helen assumed that insurers and providers of sportswear or food would enter agreements whose conditions would limit the freedom of choice between products.

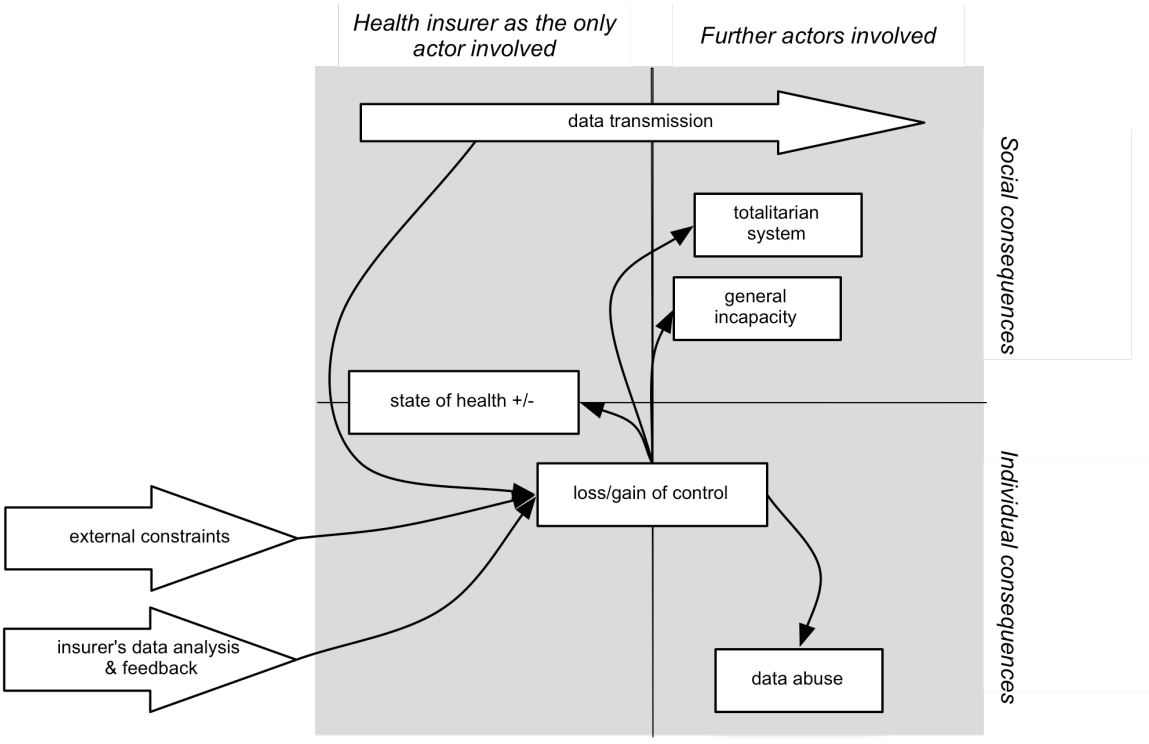


Figure 2.3. Representation B: Causal structure of the concept 'loss of versus gain in control'.

Note: Causes are displayed in arrows, consequences in rectangles.

The third cause of loss of control revealed by the data analysis was coded as 'external constraints'. This concept contained such expressions as 'constraints' (Marc) and 'constraining supervision' (Anthony). The reasons mentioned for such constraints were manifold. Apprehension was expressed that lack of money might force individuals to participate to get discounts, or that within a short time the insurer would convert the bonus system into a malus system, sanctioning non-participants with higher premiums. Furthermore, the interviewees assumed that a majority of health insurers would accept that trend and that no further technology-free alternatives would therefore be offered and that the technology would be declared legally mandatory due to the government's desire to control health expenses.

After describing the causes attributed to a loss of or gain in control, we turn now to its effects (outgoing arrows in Figure 2.3). According to the interviewees' anticipations, the result of a gain in control was a healthier lifestyle, and consequently an improved 'state of health'. Conversely, a loss of control was expected to lessen an individual's emotional wellbeing and thereby damage their state of health. For example, Anthony anticipated more 'stress' and Anne 'sadness about her own inability'.

An important further outcome of the above-mentioned delegation of responsibility for one's own state of health was seen by the interviewees as a 'general incapacity' of people, and they feared increased, uncontrollable data abuse and violations of privacy, fostering the emergence of a 'totalitarian system'.

5.3. Participating in the insurer's health program

Of further interest was the question about the circumstances under which the individual use of ubiquitous ICT might be considered. The reasons identified for participating in the health program offered or for refusing to do so, were threefold: 'cost-benefit considerations', 'participation of friends/acquaintances' and 'external constraints'.

'Cost-benefit considerations' appeared in statements such as 'personal costs are not related to the benefits' (Anthony), or 'added value of participation' (Ben). Participation was only taken into consideration if anticipated benefits outweighed anticipated costs. As shown in Figure 2.4, these considerations occurred against the background of one's own degree of (subjective) satisfaction with the current state of health (merged concept number 2146, see Figure 2.4), and the perceived need to change current practices (merged concept number 2017). A further aspect considered was the program's perceived effectiveness, depending on whether decisions about healthy lifestyles could be taken without external help (merged concept number 2317), whether the program might provide additional knowledge (concept number 711), and whether it might be helpful in new situations (concept number 1129).

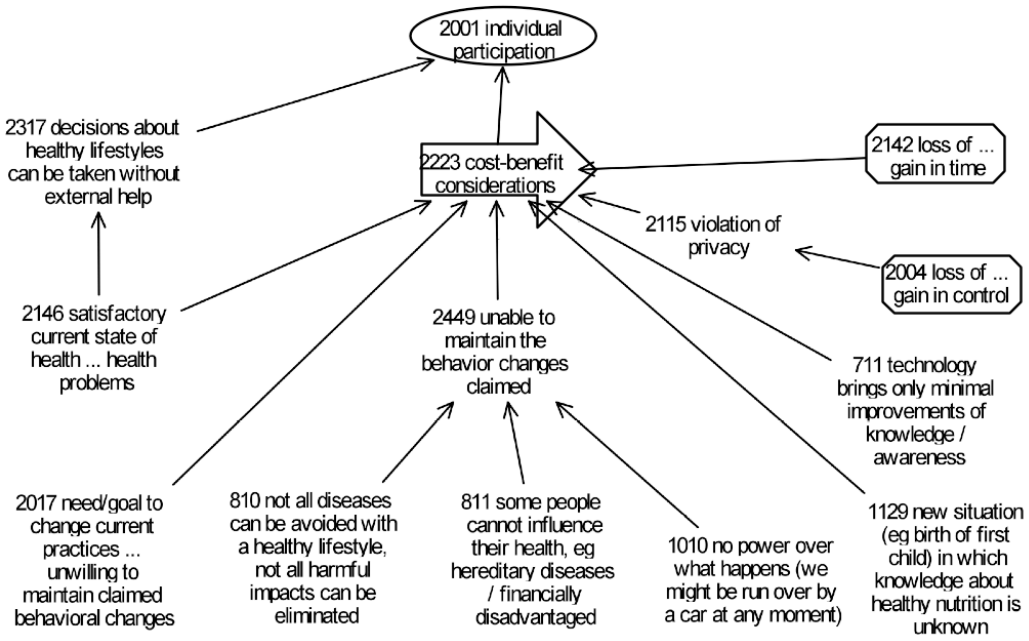


Figure 2.4. Merged reasons of the concept 'cost-benefits considerations'.

Notes: Extract from the cause map. Identified key concepts are marked in arrows (causes), rectangles (consequences) or ovals (actions). Numbers above 2000 stand for merged concepts, numbers from 100 to 1100 refer to the corresponding interviewee (cf. Appendix A). Three dots (…) divide the two poles of bipolar concepts.

Most interviewees perceived the anticipated immediate positive or negative consequences, such as a gain in or loss of time and control, as costs or benefits, respectively (illustrated in representation C in Figure 2.5). However, other interviewees also took long-term, social consequences into account. For instance, Helen and Bob feared that not all people would be able '…to maintain the behavioral changes claimed…' (merged concept number 2449 in Figure 2.4), since for some risk groups with predestined vulnerabilities, some diseases would lie beyond their control. In such a case, the interviewees expected sanctions from the insurer against those unwilling or unable to keep up a healthy lifestyle, in which case 'the insurance principle of solidarity would be driven ad absurdum' (Ben), and 'protection against control would become a luxury good' (Helen). These considerations led to negative cost-benefit considerations on their part.

The second reason to participate, the 'participation of friends/acquaintances', was characterized by statements such as 'friends and acquaintances are enthusiastic about it' (Anne), 'friends and acquaintances are participating' (Cindy, Marc), 'a highly regarded person had a good experience' (Neal). And third, the 'external constraints', presented above, turned out to foster participation.

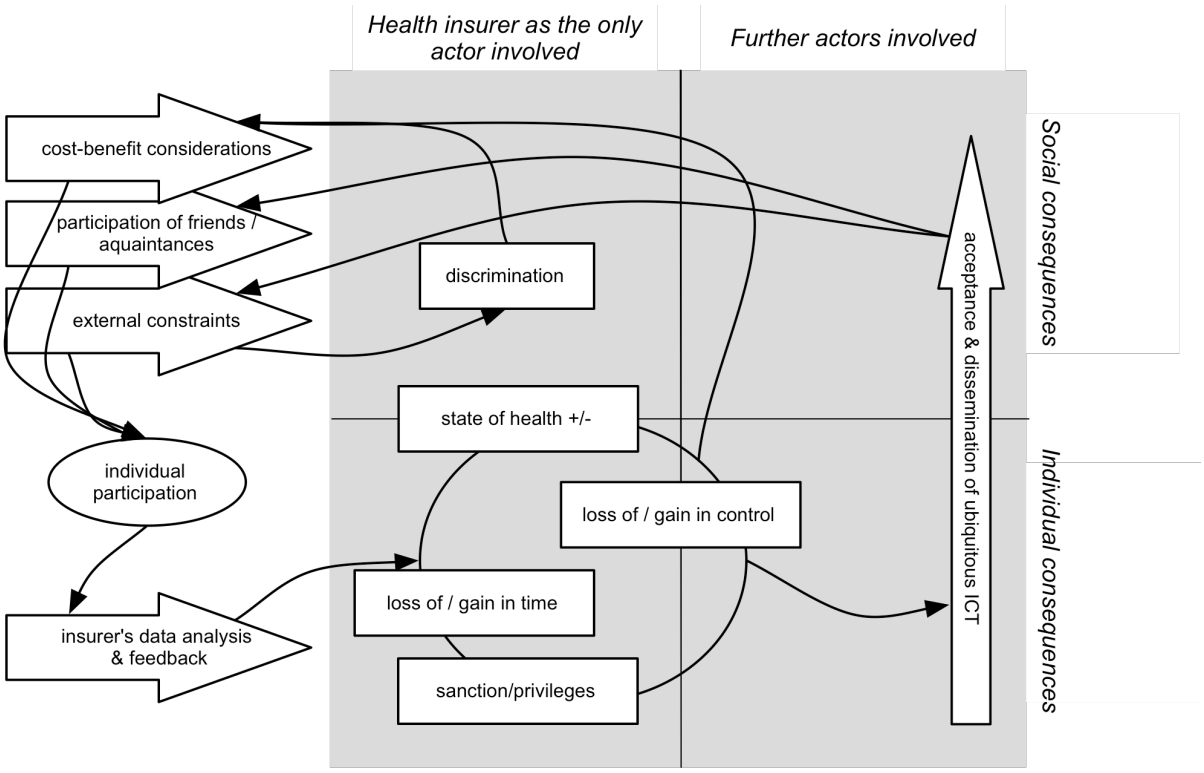


Figure 2.5. Representation C: Causal structure of the concept 'participation in the health insurer's program'.

Note: Causes are displayed in arrows, consequences in rectangles.

The anticipated causal relationships between the concepts involved indicated several reinforcing dynamic developments. First, the interviewees feared that participating might lead to a loss of control and thus to technological dependence, so that a satisfactory state of health could no longer be reached without technological support, which might foster participation. Second, although most of the interviewees rated costs higher than benefits, and consequently did not consider participating, they believed a majority of people positively evaluate ubiquitous ICT, and would thus accept and use it. This 'general acceptance and dissemination of ubiquitous ICT' was seen to enhance the impact resulting from friends and acquaintances as well as the external constraints, again emphasizing the reasons for individual participation and the discrimination against risk groups.

5.4. Changing or refusing to change health-related behavior

Furthermore, the analysis revealed that participation in the health program offered may not result in health-protecting behaviors at all. Under the term 'change or refusal to change health-related behavior', all statements were coded about behavioral adaptations due to the participation in the program. Merged original statements are displayed in Table 2-3.

Table 2-3: Merged original statements of the concept 'change or refusal to change health-related behavior'.

Interviewee	*Statements (translated from German to English)*
'Anne'	-
'Anthony'	'Inopportune behavior to the health insurer' 'Not follow the insurer's recommendations about healthy living' 'To try to avoid data transmission'
'Cindy'	'Pay attention to nutrition and exercise'
'Marc'	'Adjust own physical training' 'Unmotivated participation / refusal'
'Eric'	'Inopportune behavior, such as to drink a glass of wine' 'Cheat the system (e.g., give the sensors to my friend who is a marathon runner)' 'Found or enter an alternative social system (e.g., anarchy)'
'Ben'	'Maintain ideal bodily indicators' 'Not undertake physical training' 'Prevent data recording by putting aluminum foil around the chip'
'Michel'	'Change habits'
'Helen'	'Engaging in risky sports would no longer be possible' 'Disregard the orders (e.g., smoking)' 'Not attain the expected performance' 'Prevent data recording, boycott, cheat (e.g., not wearing the bracelet)'
'Neal'	'Enjoy something unhealthy'
'Bob'	'Drop out of the system (emigrate, enter a monastery, offer armed resistance)' 'Search for a niche in the underground' 'Emigrate / found an independent commune on an island'
'Donald'	'Lose weight' 'Stop smoking'

Original statements ranged from intended changes (e.g., Donald: 'stop smoking') to the maintenance of minimal requirements (Marc: 'unmotivated participation'), boycotting (Neal: 'enjoy something unhealthy'), and attempting to prevent or even manipulate the data recording (Bob: 'emigrate' or Ben: 'prevent data recording by putting aluminum foil around the chip').

The behavioral changes mentioned depended on the reasons for participation as shown in Figure 2.6. If participation were to be based on positive 'cost-benefits considerations', interviewees stated that they would be motivated to improve their own state of health and to use ubiquitous ICT in the intended way. Conversely, the more the participation related solely to compliance with 'external constraints' (e.g., financial pressure), interviewees would feel bothered by the feedback system, and consequently intend to avoid a real behavioral change, or even to manipulate data, thus provoking 'data abuse'. Needless to say, interviewees anticipated that their 'state of health' would improve as a result of successful behavioral changes. However, at the same time, the interviewees indicated that unmotivated or even manipulative participation,

caused by external constraints, would lead to a negative impact on people's emotional wellbeing in the form of 'emotional unease' (Michel) or 'moral conflict' (Eric). Thus, a forced behavior change was seen to harm the state of health, thereby decreasing the success of the program, slowing down technological dissemination, and, in turn, reducing the external constraints.

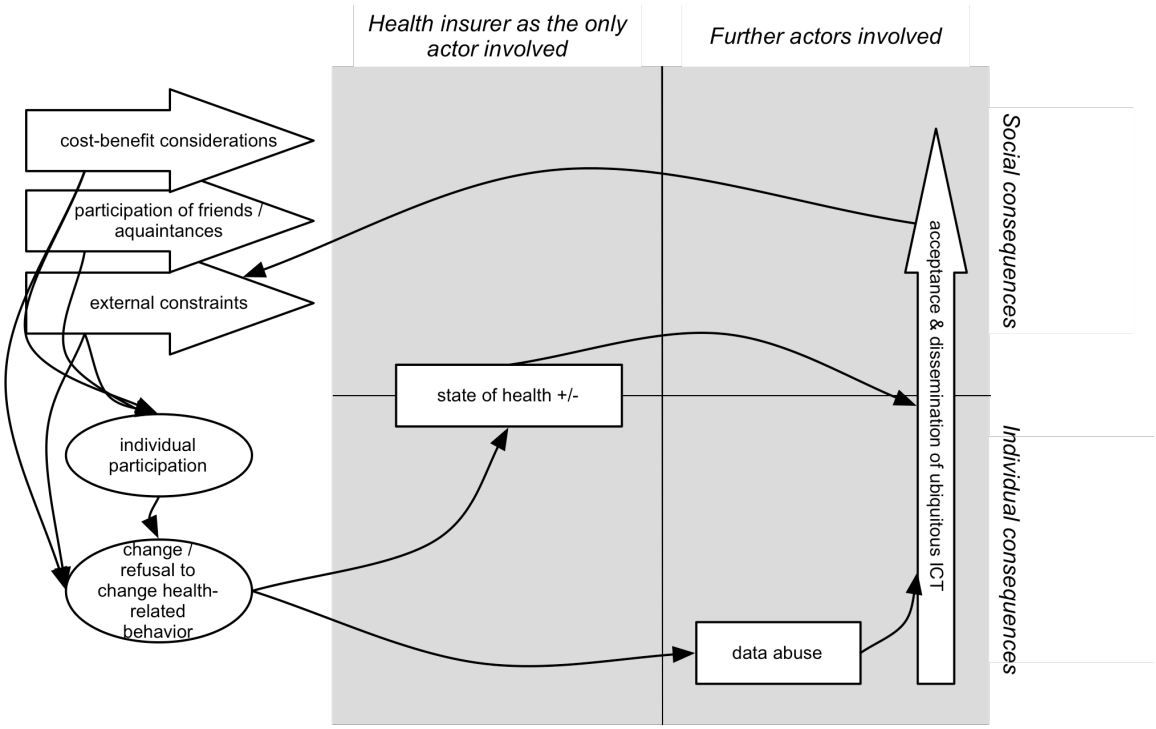


Figure 2.6. Representation D: Causal structure of the concept 'change or refusal to change health-related behavior'.

Note: Causes are displayed in arrows, consequences in rectangles.

5.5. Protective behavior options

The data analysis elicited different intended behaviors meant to prevent the negative consequences anticipated. The two most differentiated of these behaviors were 'to search for information' and 'to protest'. The intention 'to search for information' was expressed by statements such as 'gain knowledge about how the technology functions' and '… how the technology has to be employed' (Eric). Further statements included indications about potential sources of information. These were in most cases the Internet, but also '… friends with better knowledge' (Ben), '…the IT community' (Eric), '… journals, TV, radio' (Eric), and '… independent health or consumer journals' (Helen).

The exertion of protest was considered either politically, such as 'vote for a protest party' (Helen), 'deselect politicians who supported technological dissemination' (Neal), and 'to take to the street' (Neal), or in the form of 'engagement in a citizens' initiative' (Eric).

The embedding of the two behavior intentions into the overall structure is depicted in Figure 2.7. Being better informed was mentioned to support a self-controlled and self-intentioned use of the technologies, which, in turn, was seen to lead to an effective and intended improvement of one's own 'state of health'. Being informed was further supposed to counteract the 'loss of control' and the increase of a 'general incapacity', and to be a premise for further measures, such as 'to protest', with the disadvantage that staying up-to-date may demand a lot of time.

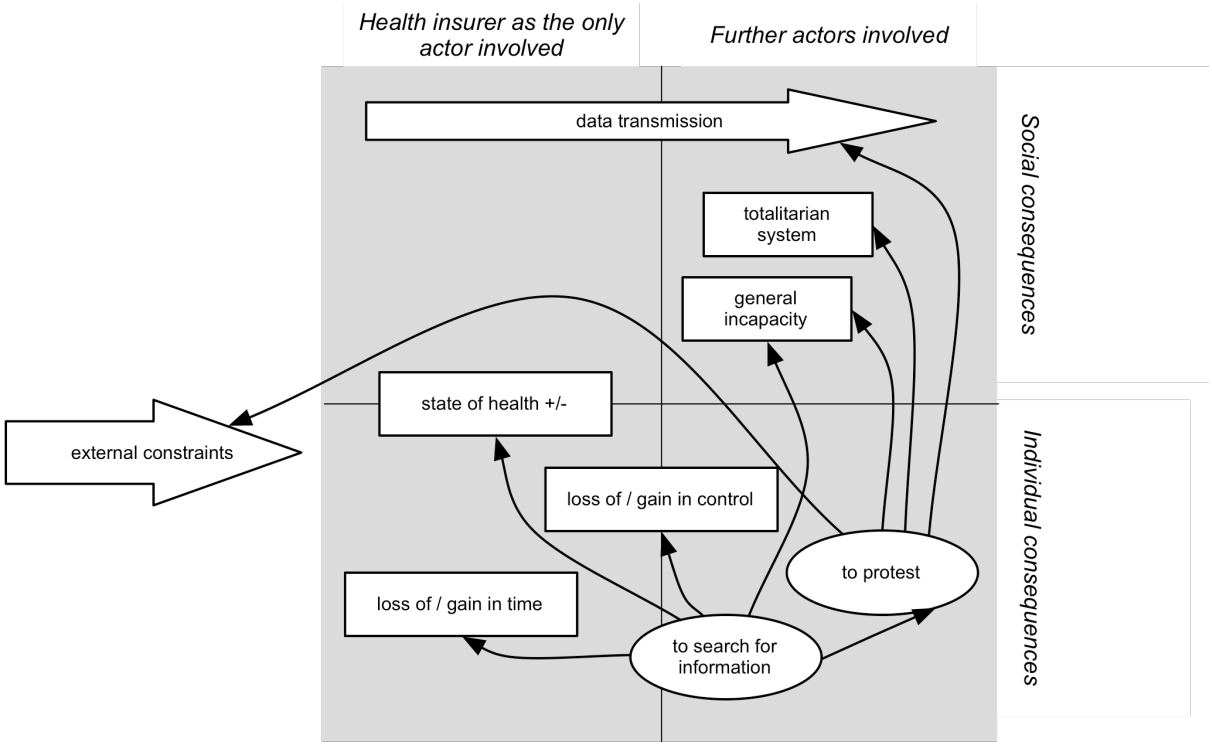


Figure 2.7. Representation E: Causal structure of the concepts 'to search for information' and 'to protest'.

Note: Causes are displayed in arrows, consequences in rectangles.

The 'search for information' was seen to enable a controlled and intentioned use of the technologies, whereas 'to protest' was rather meant to prevent inopportune causal development trends. These were the increased interconnectedness of the services, by protesting against the 'transmission of data', the emergence of 'external constraints' which force one's own participation, as well as long-term societal consequences, such as an increase in 'general incapacity' and the emergence of a 'totalitarian system'.

6. Discussion and conclusion

By eliciting the mental models of eleven interviewees, this investigation has shed light on their views about ubiquitous ICT applications in the outpatient health sector. The benefits and threats

the interviewees anticipated from the diffusion of ubiquitous ICT in the health sector can be differentiated into changes concerning individual users and changes concerning the whole society. For individual users, the interviewees expected several positive impacts, such as a gain in time and control, as well as an improved personal state of health. However, these benefits were outweighed by the expected individual and social negative consequences, such as the loss of control, inherent sanctions, the potential abuse and defectiveness of personal (health) data, as well as general incapacity and increased discrimination against citizens. These fears coincide with concerns of researchers about ubiquitous ICT applications, for example, about growing health disparities, the emergence of digital divides, inequalities between those who will benefit and those who will bear the negative consequences, loss of control, and open questions about data security and privacy (Atienza, et al., 2007; Eng, 2004; Greenfield, 2006; Skinner, Maley, & Norman, 2006; The Royal Society, 2006; Viswanath & Kreuter, 2007). Moreover, some of our interviewees' anticipation of what to expect even went beyond these predictions, such as the fear of a totalitarian system precluding all individuality or freedom, or a general incapacity on the part of citizens.

The main drivers for such an unfavorable development were said to be an abusive handling of confidential data, and the pervasion of all ubiquitous ICT into all areas of life due to improvident adoption. These concerns reflect a certain institutional distrust (R. E. Kasperson, Golding, & Tuler, 2005). For example, the interviewees mentioned a lack of trust due to insufficient technological safety, expressing concerns about data defects, abusive data intrusion by a third person (data hacking), and assumptions about the ease of unauthorized data manipulation. Additionally, a lack of trust in the provider of the program was observed; interviewees assumed that profit-driven health insurers would sell data and transform the program into a malus system as soon as the social participation was sufficiently high. Moreover, interviewees did not trust the government to enact reliable data-protection laws in time. In fact, the government was assumed to have a particular interest in an increased control of its citizens, and therefore to actively foster the diffusion of ubiquitous ICT in the health sector or to enforce legal access to citizens' data. And finally, there was no trust in a self-regulating market. On the contrary, interviewees believed that their fellow citizens would improvidently adopt new technologies, and thereby reinforce normative influence and external constraints.

As initially outlined, ubiquitous ICT applications are expected to support the maintenance of a healthy lifestyle (Neuhauser & Kreps, 2003). The results indicate that success in this domain may depend on the user's favorable evaluation of the technology; only if the expected benefits of an application outweighed anticipated costs (individual as well as societal) did interviewees intend to use the technology in an appropriate way. Interviewees made their evaluation in line with their underlying satisfaction with their own health. In other words, only if interviewees were already aware that their own state of health should be improved and were motivated to undertake the needed behavioral changes was the use of ubiquitous ICT more closely consid-

ered. Attributes of ubiquitous ICT intended to support behavioral changes, like tailored information and feedback, were perceived as annoying or even disturbing if there was no intrinsic motivation for healthier lifestyle modifications. In line with this is the assertion of Fogg (2003) who claims, that only those technologies that support people in achieving their individual goals are evaluated positively. Conversely, as the results indicate, forced diffusion by extrinsic 'motivators', such as the restriction of choice or financial or legal pressure, seem to be completely counterproductive regarding behavioral change. Forcing individuals to participate, especially if done by government or industry, may lead to reactance and unintended adverse effects, such as technological refusal or data manipulation. This is crucial because experts have agreed that ICT technologies in the health sector will only be disseminated by commercial ventures and sales or financial support from foundations (Eng, 2004).

In regard to potential protective reactions against the negative consequences of the diffusion of ubiquitous ICT, only unspecific intentions were identified, such as the search for information and the willingness to protest. In fact, the interviews were shaped by a certain feeling of helplessness, reflected in the key concept 'loss of versus gain in control'. Thus, a better understanding of how individual protective behavior could be aroused and supported is essential.

However, these interpretations must be viewed with a certain degree of caution. First of all, only accessible thoughts can be acquired by exploring mental models (Doyle & Ford, 1998). Unconscious representations (implicit models) remain beyond comprehension. Furthermore, mental models present what people think, but not why, i.e., they do not provide direct insights into mental processes (Rouse & Morris, 1986). Thus, mental processes should be investigated with other procedures. Caution is also advised as to the generalization of the findings. Despite the diversity of the concepts, we are aware that the variety of personal parameters of the sample, such as the age range, is rather low. Moreover, the sample did not include any interviewees with severe health problems. Those suffering from a disease may have looked at the current development from a patient's perspective and their hope for a better future may have affected their opinion differently than those from a healthy sample.

The study of the public impacts of ubiquitous ICT in the outpatient health sector is in its infancy. Clearly, much more research needs to be conducted in this area. Nevertheless, the findings gave rise to the hypothesis that the diffusion and implementation of ubiquitous ICT will only succeed if the problems of mistrust and cost-benefit appraisal, as discussed above, are addressed. This can be accomplished by evaluation, communication, and participation (The Royal Society, 2006). The evaluation of ubiquitous ICT applications in the health sector is a widely expressed need (Glasgow, 2007). Eng et al. (1999) call for strict control mechanisms of new ICT applications similar to those for drugs and medical devices, demonstrating their safety and effectiveness before approval. Only a serious assessment of the impacts of ubiquitous ICT may guarantee quality, utility, and effectiveness. Communicating these evaluations may then promote public confidence

and increase their ability to deal with risks appropriately. However, communication should not only flow from experts to citizens, but also in the reverse direction from citizens to experts (Pidgeon & Rogers-Hayden, 2007). The early participation of user groups in the product-development life cycle may inspire trust and separate the technological wheat from the chaff, thereby maximizing the utility and usability of future ICT technologies in the outpatient health sector so as to minimize their risks.

Chapter 3:
A Structural Equation Model Explaining Responses to the Threats of Ubiquitous Information and Communication Technologies

This chapter is an early version of an article published as: Moser, S., Bruppacher, S.E., & Mosler, H.-J. (2011). How people perceive and will cope with risks from the diffusion of ubiquitous information and communication technologies. *Risk Analysis, 31*(5), 832-846.

Abstract

Information and communication technologies (ICTs) are increasingly pervasive and continue to reshape our environment. This trend carries different risks. Therefore, the early sensitization of people to these risks, as well as improving their capacity for protective coping behavior, is essential. Based on the Protection Motivation Theory (PMT), with structural equation modeling, the relationships between different components of threat and coping appraisal were examined to explain protective and non-protective responses. Calculations were performed with data from a representative survey on the perception and use of ICT among German residents (N = 5030). The findings largely supported the proposed model: an increased perceived threat was positively related to the intentions to react protectively and non-protectively. Perceived coping efficacy increased the protective and decreased the non-protective responses. Negative affect enhanced the perceived threat and the non-protective response, but inhibited protective intentions. The implications of these findings on how to sensitize people to the risks of these new technologies are outlined.

Keywords: Protection-Motivation Theory, Risk Perception, Threat Appraisal, Coping Appraisal, Ubiquitous Information and Communication Technologies

1. Introduction

Rapid advances in the field of information and communication technologies (ICTs) have fundamentally changed our lives. There is no evidence that the ongoing trend of producing smaller, cheaper, and more powerful microprocessors and storage components will decelerate in the near future (G. E. Moore, 2003). We can expect personal computing (i.e., one computer per person) to be replaced by the omnipresence of interconnected mini-computers. Weiser (1991) promised in his vision of 'ubiquitous computing' a life in which our tasks are powerfully assisted by invisible computers, embedded in everyday objects and functioning anywhere at anytime. A famous prospective application of ubiquitous ICT is the 'smart home,' e.g., furnished with an intelligent refrigerator that recognizes its contents thanks to radio frequency identification (RFID) tags. Thereby, it identifies missing articles and automatically orders them via the Internet.

Such scenarios may sound unrealistic, but the first steps in this direction have already been implemented: multifunctional mobile phones, GPS, WLAN, RFID tags, and so on, are a reality; for many people, they are indispensable. Proponents of the vision of ubiquitous computing promise enhanced convenience and safety, lower administrative costs and more free time, since technology will release users from everyday burdens. It is also seen to help conserve natural resources, and recognized for its immense market potential for the IT and telecommunication industries (Greenfield, 2006; ITU, 2005, 2006; Mattern, 2005).

The technological penetration of our daily lives will not only lead to positive effects. Kruse (1981) has warned that we shall have to pay the price for technological facilitations in the form of reduced data safety, loss of privacy, or the loss of control over the profile that we communicate (unintentionally) to others. In light of ongoing technological changes, these concerns are much more prevalent than they have ever been. Experts are concerned about the increased power consumption and exposure to non-ionizing radiation, the (uncontrollable) complexity, non-distinctive responsibilities and legislation, the loss of privacy, undermined data protection, discrimination due to filed data profiles, and an emerging divide (called the digital divide) between those who profit from these new technologies and those who are unwilling or unable to participate, and thus will only suffer the negative consequences (Greenfield, 2006; Lyon, 2001; Som, et al., 2004; Stajano, 2003; Stone, 2003).

Kruse (1981) proposed the encouragement of people's capacities to prevent technological strain. Thus, people should acquire skills and capabilities to handle the technological environment in a competent, intended, and self-determined way. They should be able to keep up with the developments and control the technology instead of being controlled by it. This study aimed at contributing to the question of how this could be supported in an effective way. A premise for a competent coping with the adverse effects of ubiquitous technologies is people's motivation to

take protective actions. Part of the building of this motivation rises through people's assessment of how the technology threatens them, and what resources they have on hand to deal with this threat. An adequate theoretical framework that combines the appraisal of threat with the appraisal of coping alternatives to explain the formation of a protection motivation is offered by the protection motivation theory (PMT) (Rogers, 1975, 1983). In order to better understand how the acquisition of technology-related competencies might be supported and how the feelings of technological overstrain might be prevented, a survey was conducted and a model tested that was based on the theoretical implications of the PMT. In particular, the following questions were addressed:

- What components impact people's appraisal of threats of ubiquitous ICT and their perceived coping efficacy to deal with these threats?
- To what extent do the perceived threat and coping efficacy predict the intentions to take protective actions against these threats?
- To what extent do the perceived threat and coping efficacy predict undesirable responses, such as technological overstrain, helplessness, and denial?
- How does negative affect influence the choice between protective and non-protective responses?

2. Appraisal of and coping with threats

Protection Motivation Theory (PMT) (Rogers, 1975, 1983; Rogers & Prentice-Dunn, 1997), the theoretical basis of this survey, was originally introduced as a framework to explain health-related behavior (e.g., smoking; Maddux & Rogers, 1983), as well as to predict the efficacy of health behavior interventions (e.g., stop smoking campaigns; Pechmann, Zhao, Goldberg, & Reibling, 2003). Following Lazarus' (1966) classical theory of psychological stress, PMT assumes health-threatening information (coming from environmental or intrapersonal sources) to activate two mediating cognitive processes. The first is the threat or risk appraisal, whereby the threat is evaluated with respect to its severity and vulnerability. Severity refers to the degree of the expected harm of the feared negative event (Rogers & Prentice-Dunn, 1997), while vulnerability is defined as the probability of occurrence of an event, given the persistence of an existing behavioral disposition and the omission of protective actions (Rogers, 1975). The severity and vulnerability assessments interact with the evoked fear, and are reduced by perceived intrinsic and extrinsic rewards of the unhealthy behavior. The second mediating process comprises the coping appraisal, through which different threat-reducing behavior alternatives are assessed based on their feasibility (self-efficacy), response efficacy, and on possible costs and barriers. With an increase in perceived threats, the protection motivation becomes stronger, which in-

cludes the following alternatives: Given a positive coping appraisal, people engage in threat-reducing attitudes, intentions, or actions. Where no behavior alternative is perceived as reliable, people lapse into non-protective responses. The stress resulting from the threat is reduced by downplaying the threat or their own involvement (avoidance, denial, wishful thinking), or by falling into helplessness or hopelessness (Peter & Kaufmann-Hayoz, 2000; Rippetoe & Rogers, 1987; Witte, 1998).

Fragments of PMT have been empirically tested (for an overview, see e.g., Rogers & Prentice-Dunn, 1997). Floyd and Prentice-Dunn (2000) found in their meta-analysis significant impacts of severity, vulnerability, and rewards as well as of response efficacy, self-efficacy, and response costs of health-related intentions and actions. In their meta-study, Milne, Sheeran, and Orbell (2000) revealed high predictive validity of all three components of the coping appraisal process on health-related intentions and behaviors, but found a rather poor predictive power of the components of the threat appraisal process. Although PMT was originally proposed to explain people's responses to health threats, potential applications also imply a broader context: Gardner and Stern (1996) modified the theory to explain human behavior regarding environmental threats and technological hazards. These authors added the concept of values to the threat-appraisal process, thereby extending the range of applications from perceived personal threats to perceived threats of anthropocentric and biocentric values. Empirical applications of the PMT outside the field of health psychology are less common: Martens and Rost (1998) investigated complex, multivariate relations to explain 10 different direct environment behaviors (e.g., to abandon the car) and indirect environment behaviors (e.g., participation on an action day to reduce garbage). They found that a high motivation to act pro-environmentally could be explained with high severity, high vulnerability, the type of the personal coping style, and low trust in authorities and industry. The behavior choice was, for its part, defined by the motivation to act pro-environmentally, high self-efficacy, and high response efficacy. In four studies, Homburg and Stolberg (2006) assessed private sphere environmentalism, non-active public sphere environmentalism, and pro-environmental behavior in workplaces. These behaviors were predicted by protective responses such as searching for information, which, in turn, was predicted by demand appraisal (comprising threat and harm), and collective self-efficacy. Grothmann and Reusswig (2006) identified threat experience, trust in public flood protection, coping appraisal, non-protective responses, and (although somewhat weaker) threat appraisal to be significant predictors of diverse precautionary actions with respect to flooding. Rochford and Blocker (1991) found that the appraisal that flooding could be controlled was negatively related to an emotion-focused coping style and positively related to a problem-focused coping style as well as to the involvement in protest activism.

In contrast to the well-documented effectiveness of the above-described predictors, research following the PMT has so far given only minor importance to the role of fear (Eagly & Chaiken,

1993). This concept was empirically neglected and theoretically ambiguous: Following Rogers' (1983) conception, fear interacts with severity and vulnerability, and at the same time predicts the protection motivation. However, in Gardner and Stern's (1996) adaptation, fear generally interacts with the perceived threat. Conversely to its vague specifications in the PMT, the literature on risk perception and evaluation accounts for various functions of fear, or 'negative affect' evoked by threatening stimuli. First, affect may serve as information or cue for risk judgments. As the 'affect heuristic' of Slovic and colleagues (2002, 2004) suggests, people base their risk judgments not exclusively on cognitively processed information, but also on their feelings toward the stimulus. The impact of the affect on the risk judgment increases when cognitive risk information is not available or too complex.

Second, affect may directly serve as a motivator of certain risk-reducing behaviors (De Hoog, Stroebe, & De Wit, 2007; Loewenstein, Weber, Hsee, & Welch, 2001; Peters, Lipkus, & Diefenbach, 2006). It was found that anxiety triggered avoidance (Cameron, 2003), anger provoked the intention to boycott the originator of the damage (Karger & Wiedemann, 1998; Nerb, Spada, & Wahl, 1998), and fear enhanced non-protective responses (Lerner & Keltner, 2001; Loewenstein, et al., 2001; Rippetoe & Rogers, 1987).

Besides the PMT variables, two further constructs related to threat appraisal were included in this survey. The first is 'institutional trust': It is assumed that people perceive less threat if they believe that institutions such as the legislator, NGOs, or ICT producers undertake effective protection activities. Enhanced trust decreases self-responsibility for individual protective actions (Grothmann & Reusswig, 2006; Kuttschreuter, 2006; Siegrist, 2000; Siegrist, Cvetkovich, & Roth, 2000). Trust seems to influence risk judgments, especially in situations where knowledge is lacking, or when people need to reduce complexity (Siegrist, 2000).

The second construct is the role of 'previous experiences'. PMT stipulates that previous negative experiences with similar threats increase the perceived threat. Empirical findings support this postulation (Grothmann & Reusswig, 2006; Siegrist & Gutscher, 2006). On the other hand, the number of previous experiences with the threat-evoking object seems to decrease risk perception. Kuttschreuter and Gutteling (2004a) found that frequent computer users perceived the risk of a millennium bug at the turn of the millennium as significantly lower than people with scarce computer experiences. Furthermore, the group of experienced users rated their ability to cope with the millennium bug higher, and was better informed than non-experienced people for whom the topic was rather unfamiliar.

3. Model conception

Based on the considerations outlined above, we hypothesized a model that explained different responses to the perceived threat of ubiquitous ICT (Figure 3.1): Perceived threat was expected

to correlate positively with protective as well as with non-protective responses; the perceived coping efficacy was expected to correlate positively with protective responses, but negatively with non-protective responses (Gardner & Stern, 1996; Rogers, 1983). Perceived threat was operationalized on the level of threatened anthropocentric and biocentric values following Gardner and Stern's (1996) conceptualization. We believed further that the anticipated personal susceptibility in the sense of Rogers (1983) may impact the perceived threat. Thus, the anticipated personal susceptibility was expected to correlate positively with the perceived threat.

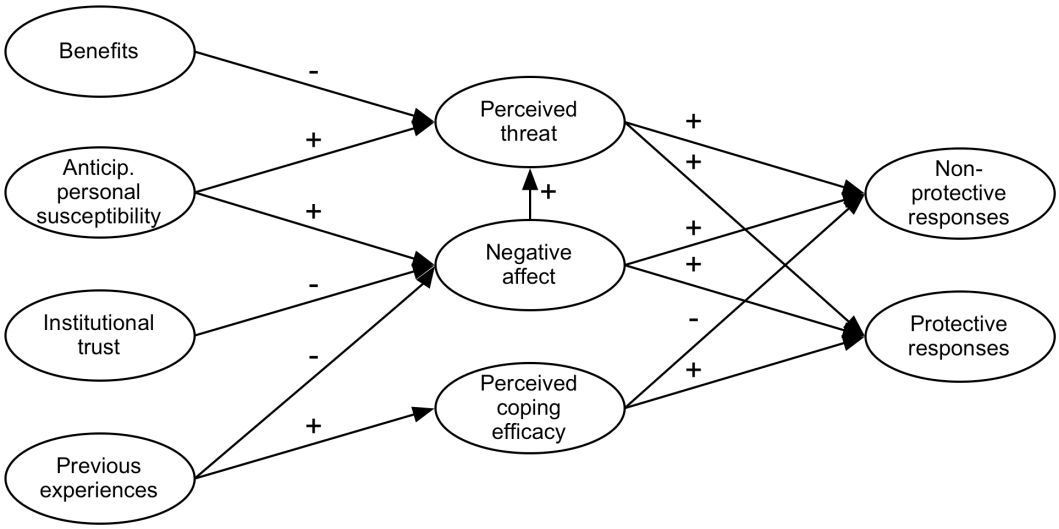


Figure 3.1. Hypothesized conceptual model, explaining protective and non-protective responses based on the protection motivation theory (PMT).

According to the assumption of the PMT that perceived rewards reduce the perceived threat (Rogers, 1983; Rogers & Prentice-Dunn, 1997), a negative relation was assumed between perceived benefits of ubiquitous ICT and the perceived threat.

Furthermore, negative affect was assumed to serve as a cue for the threat appraisal and thus to correlate positively with the perceived threat (Slovic, et al., 2002, 2004). Additionally, negative affect was expected to function as a direct motivator for the protective as well as for the non-protective responses, thus to correlate positively with both of them (De Hoog, et al., 2007; Loewenstein, et al., 2001; Peters, et al., 2006).

Negative affect, in turn, should decrease with high institutional trust (Earle & Cvetkovich, 1995; Siegrist, et al., 2000) and increase with anticipated personal susceptibility (Kuttschreuter, 2006). Thus, a positive correlation was assumed between anticipated personal susceptibility and negative affect, and a negative correlation was expected between institutional trust and negative affect.

Finally, we believed that people with a wide range of previous experiences with the existing ICTs would react with lower negative affect to technological threats and with higher coping efficacy

than people with a lack of experience (Kuttschreuter & Gutteling, 2004a). With regard to previous experiences, therefore, a negative correlation with negative affect was assumed, and a positive correlation with the perceived coping efficacy was expected.

4. Method

4.1. Procedure and respondents

The data used to test the model described above were derived from a survey on the use and perception of current and future ICT. The conception of the survey was cooperatively undertaken within the research cooperation (cf. section 5 in chapter 1) under the lead management of our research partner 'Sinus Sociovision'. The data collection took place from March to May 2007 in Germany and was accomplished by an opinion research center. The sample was selected with the ADM master-sampling method, a multi-level selection procedure for random sampling in Germany's German-speaking resident population (for a detailed description of the method, see Behrens & Löffler, 1999). The first selection step involved the random selection of 258 sampling points, which were based on the German electoral districts. In the second step, with the help of the random route procedure, households inside the sampling points were randomly identified and visited by professional interviewers. And third, the interview partners were randomly selected out of all family members older than 14 years and invited to participate. Face-to-face interviews were conducted in the home of the interviewee, with the help of a standardized questionnaire. Interviewees were financially compensated for their participation. A total of 5,030 people were interviewed. The mean age of the interviewees was 47.3 years (SD = 18.4), and 48% were men. Thirteen point six percent of the interviewees had higher education qualifications, 8% had finished polytechnic grammar school (in the former GDR), 26.9% had completed secondary school, 42.4% had elementary schooling, and 1.1% had not completed schooling (7.9% missing data). About 5.2% of the interviewees were self-employed/freelancers, 46.3% were employees, 3.8% worked in the public sector, 32.2% were unskilled and skilled workers, and 0.7% were farmers (11.8% missing). Monthly net household incomes varied from less than 500€ in 1% of the cases, 500–1,000€ in 6.3%, 1,000–1,500€ in 17.1%, 1,500–2,000€ in 19.4%, 2,000–2,500€ in 19.3%, 2,500-5,000€ in 31.6%, to above 5,000€ in 4.2% of all cases (1.2% missing data).

4.2. Measures

The standardized questionnaire, originally in German, first assessed the current use of different ICTs, as well as their subjective importance to the user. The second section evaluated prospec-

tive ubiquitous ICT, the third section concerned preferences of information channels, the fourth section investigated potential coping alternatives, and the last section assessed demographic information. Items used to estimate previous experiences with ICT stem from the first section of the questionnaire. Items to assess benefits, anticipated personal susceptibility, institutional trust, negative affect and perceived threat were derived from the second section. Items relating to the appraisal of coping, the protective responses and the non-protective responses were assessed in the fourth section of the questionnaire. An overview of the English translation of all items used in the analysis and the introductions to the different sections is presented in Appendix B. If not indicated otherwise, the items were ranked using a 4-point scale (from 'completely right' to 'completely wrong'). They were explicitly formulated for this investigation and based on substantial qualitative pilot studies (described in chapter 2 and in Wippermann, 2007). Due to the early implementation stage of this research, reasonable individual protective responses against the risks of ubiquitous ICT were difficult to name. However, on the basis of the piloting (cf. chapter 2), two protective response alternatives were identified which are already realizable for a general public. These are the 'intention to search for information about ubiquitous ICT' (operationalized with three items, e.g., 'I will check on who has access to the data stored by means of modern ICT'), and the 'intention to take political actions' against the risks of ubiquitous ICT (two items, e.g., 'I will take political actions against the pervasion of our life by modern ICT'). These two response alternatives entered the statistical model as two separate constructs.

To assess the perceived coping efficacy, items covering the self-efficacy ('I know how to find credible information on the development and consequences of modern ICT,' and 'I am capable of taking political actions'), and items covering the response efficacy ('I believe that checking on the developments and consequences of modern ICT is an appropriate action to lower their risks' and 'I believe that taking political actions is an appropriate action to work against their risks') were formulated according to the above-described response alternative. Thus, two distinct constructs, one appraising the efficacy of information-seeking and one appraising the efficacy of political actions, composed of two items per construct (evaluation of self-efficacy and response efficacy), entered the statistical model.

The non-protective response was measured with the four items 'overstrain' ('In an everyday life which is pervaded with interconnected ICT, I will be overstrained'), 'general denial' ('Ubiquitous ICT will never exist'), 'denial of personal susceptibility' ('Potential risks of an everyday life pervaded by modern ICT will not affect me') and 'helplessness' ('We cannot do anything against the risks of new technologies').

Perceived threat was covered with the three subscales 'ecological threats' (three items, e.g., 'Because computers, scanners, chips, etc. require material, important natural resources will not be available anymore.') referring to endangered biocentric values, 'social threats' (eight items, e.g.,

'Human behavior will be more and more controlled') referring to endangered anthropocentric values, and 'general threats' (two items, e.g., 'The future omnipresence and interconnectedness of ICT will provoke severe problems').

Negative affect was assessed twice with the questions 'I have an uneasy feeling about what is approaching us,' and 'I am scared by the variety of ICT functions.'

Benefits were measured with nine items, such as 'Devices with key memory / automatic personalization will be easier to use.' Anticipated personal susceptibility was measured with two general items (e.g., 'My behavior will be observed'), three items referring to ICT applications in the health sector (e.g., 'Due to the data storage, my patient rights are at risk') and two items referring to applications in the purchasing sector (e.g., 'I suspect that data about my shopping behavior will be handed to unauthorized persons').

Two items assessed the institutional trust in the legislator (e.g., 'The government will release laws to prevent hazards of future ICT'), three items covered the trust in technology suppliers and the free market (e.g., 'I fully trust in the organizations that collect sensitive data to responsibly deal with them'), and two items measured the trust in other institutions (e.g., 'Concerning the risks of modern ICT, I fully trust in consumer protection organizations').

Previous experiences with ICT were assessed in four ways. The interviewees were presented with a broad list of the existing ICT applications (e.g., desktop computer, laptop/notebook, smart phone, etc.); they then had to indicate which of these applications they used privately and/or professionally (multiple answer alternatives). The responses were summed up to obtain ratings of private and professional uses. Then, the interviewees were asked about the frequency of mobile phone use (one 5-point scaled item), and finally, about the frequency of Internet use (four 5-point scaled items covering Internet use at home, in the workplace, at school or university, and elsewhere, e.g., Internet corner).

In the early stages of research, a Cronbach's α coefficient of >0.70 is considered as acceptable as the cut-off criterion for internal consistency of a scale (Garson, 2009; Nunnally & Bernstein, 1994; Streiner, 2003b). However, it is known that Cronbach's α coefficients increase with the number of items per scale; therefore, we regarded the more lenient criteria of >0.60 as sufficient for two-item scales. From Table 3-1, it can be seen that the scales met the criteria with one exception: the items covering different variants of non-protective responses showed only low reliability (α = 0.45). This stands in contrast to the high intercorrelation findings of Witte (1994; 2000), who treated the different non-protective response alternatives as one construct. In the present case, the 'non-protective response' seems to possess the structure of an indicator rather than the one of a unidimensional scale (cp. Streiner, 2003a). The implications of this structural discrepancy will be discussed later.

4.3. Data analysis

To test the outlined conceptual model, a structural equation model (SEM) was calculated, using the software AMOS 16.0. The variance-covariance matrix served as input (missing listwise, the correlation matrix can be found in Appendix C); calculations were run using the method of maximum likelihood estimation (ML). For scales with more than four items (e.g., the latent variable 'benefits'), the items were aggregated to parcels by taking the mean of several items. Using these parcels as indicators allowed the number of the estimated parameters to be kept low (Bagozzi & Edwards, 1998; Little, Cunningham, Shahar, & Widaman, 2002). For all other scales, the two to four single items were used as indicators. An overview of which items entered which indicators is given in Appendix B. Structural equation modeling offers the possibility to test, with multiple indexes, the goodness-of-fit of the tested model with its underlying data. For the evaluation of the proposed model, the recommendations of Bollen and Long (1993), Bryne (2001), and Hu and Bentler (1998, 1999) were followed, by considering the following indexes with the following conventional cut-off criteria as acceptable: Comparative Fit Index (CFI) > 0.90, Root Mean Square Error of Approximation (RMSEA) < 0.06, and Standardized Root Mean Square Residual (SRMR) < 0.08. We further report the models' χ^2; however, due to the well-known problem of rejection of true models in view of large sample sizes (Schumacker & Lomax, 2004), this index was expected to be inconclusive. For path coefficients, a significance level of $p < 0.01$ was applied.

5. Results

A total of 4,817 cases entered the data analysis, 213 (4.2%) cases had to be excluded due to missing data.

5.1. Test of the measurement model

The calculation of a confirmatory factor analysis (CFA) permitted, in a first step, the goodness-of-fit of the measurement model with the underlying data to be tested. Therefore, all latent constructs were allowed to correlate with each other. By doing this, the structural model corresponded exactly to the covariance matrix and the resulting fit indices thus reflected the deviations between the measurement model and its data basis. The resulting fit indices were satisfactory: χ^2 = 4,674.73, df = 379, $p < 0.001$, CFI = 0.94, RMSEA = 0.049 (90% confidence interval 0.047–0.050), SRMS = 0.0453.

The detailed examination of the factor loadings and explained variances of the indicators (shown in Table 3-1) revealed all factor loadings to be significant ($p < 0.001$). The indicators

were adequately represented by their underlying factors, again with the exception of the construct 'non-protective response'. This factor was overrepresented by the indicator 'overstrain', as can be concluded due to the low explained variances and factor loadings of the other three indicators 'helplessness,' 'personal denial,' and 'general denial.'

Table 3-1: Overview of the measurement model

Latent construct	*Indicator*	*r*	*R^2*	*α*
Previous experiences with ICT	Professional	.60	.36	.84
	Private	.82	.67	
	Internet	.82	.68	
	Mobile phone	.67	.45	
Anticipated personal susceptibility	General	.61	.38	.78
	Health	.55	.30	
	Purchase	.65	.43	
Institutional trust	Other institutions	.73	.53	.82
	Legislation	.82	.66	
	Free market	.77	.59	
Benefits	Benefits 1	.88	.77	.88
	Benefits 2	.81	.66	
	Benefits 3	.91	.82	
Negative affect	Unease	.75	.56	.71
	Scare	.74	.54	
Perceived threat	Ecological risks	.63	.39	.89
	Social risks	.89	.79	
	General risks	.78	.61	
Non-protective response	Overstrain	.76	.58	.45
	General denial	.23	.05	
	Denial of personal susceptibility	.27	.07	
	Helplessness	.33	.11	
Intention to search for information	New developments	.86	.74	.87
	Functioning	.92	.84	
	Access	.75	.56	
Perceived coping efficacy for information seeking	Response efficacy	.63	.40	.65
	Self-efficacy	.77	.59	
Intention to take political actions	Pervasion of life	.69	.48	.67
	Avoid future risks	.72	.52	
Perceived coping efficacy for political action	Response efficacy	.63	.39	.68
	Self-efficacy	.82	.67	

Notes. r = standardized factor loadings, R^2 = explained variances, α = Cronbach's alpha coefficient. All factor loadings $p < 0.001$.

5.1. Explanation of protective and non-protective responses (Test of the structural model)

To test the hypothesized relationships, the correlations between the latent constructs in the above-described measurement model were replaced by the hypothesized regressions. The independent variables and the error terms of the dependent variables were allowed to correlate. The correlations among the dependent variables are based on the assumption that a restriction to zero (= no correlation) is not justified, since they are explained by the same predictors. Thus, at least a small commonality can be expected. The model showed promising fit indices: χ^2 = 5659.87, df = 406, $p < 0.001$, CFI = 0.92, RMSEA = 0.052 (0.051–0.053), SRMS = 0.0529, (fit indi-

ces for the model without correlations among the dependent variables are: χ^2 = 5861.24, df = 409, p < 0.001, CFI = 0.92, RMSEA = 0.053 (0.051–0.054), SRMS = 0.0525).

The structural examination revealed insights into the predictive structure of the non-protective and protective responses and mainly confirmed the expectations. As visualized in Figure 3.2, the non-protective response varied, as hypothesized, with the 'perceived threat' (β = 0.24, p < 0.01), the 'negative affect' (β = 0.36, p < 0.01), and the perceived coping efficacy of information-seeking (β = –0.36, p < 0.01). In contrast, and against expectation, the perceived coping efficacy of political actions did not impair the non-protective response (β = 0.02, p = 0.39). These four predictors together explained 61% of the variance of the non-protective response.

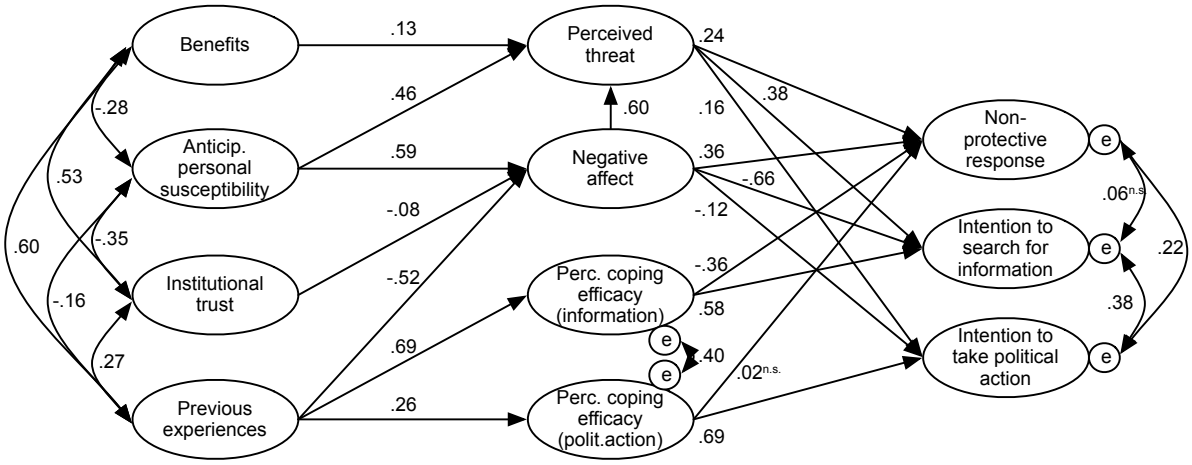


Figure 3.2. Standardized regression and correlation coefficients for the structural model predicting the non-protective response and the two protective response alternatives (intention to search for information and intention to take political action).

Notes. χ^2 = 5659.87, df =406, p < 0.001, CFI = 0.92, RMSEA = 0.052 (0.051–0.053), SRMS = 0.0529, p < 0.01 for all standardized path coefficients and correlations, if not marked otherwise. For reasons of clarity, the indicators and factor loadings were omitted.

The explained variance of the first protective response alternative, i.e., the intention to search for information, was 0.70. The perceived threat and coping efficacy fostered information-seeking as predicted (β = 0.38 and 0.58, p < 0.01); however, against expectation, the 'negative affect' exerted a strong impeding effect (β = –0.66, p < 0.01).

The same, though much weaker negative relation, was found between 'negative affect' and the 'intention to take political actions' (β = –0.12, p < 0.01). The main factor altering this second protective alternative (R^2 = 0.49) seemed to be its perceived coping efficacy; the perceived threat played a minor role (β = 0.69 and 0.16, p < 0.01).

Previous experience with ICT influenced both the perceived efficacy to search for information (β = 0.69, p < .01, R^2 = 0.47) and – to a somewhat lower degree - the perceived efficacy of political

action (β = 0.26, p < .01, R^2 = 0.07). The correlations of 0.40 and 0.38 (both p < 0.01) between the error terms of the two protective response alternatives and between the error terms of the corresponding coping efficacies indicated that reaction patterns of these two response options are similar. Whereas the intention to act politically and the non-protective response seem to coexist (r = 0.22, p < 0.01), the non-protective response and the intention to search for information were not related (r = 0.06, p = 0.073).

As expected, the 'negative affect' (R^2 = 0.77) was altered by the 'anticipation of personal susceptibility,' and was decreased by the reference to 'institutional trust' and the availability of 'previous experiences' with ICT (β = 0.59, –0.08 and –0.52, p < 0.01). 'Negative affect', for its part, increased the perceived threat (β = 0.60, p < 0.01), and the same was the case for the 'anticipated personal susceptibility' (β = 0.46, p < 0.01). Contrary to expectation, the perceived 'benefits' were not negatively related to the perceived threat (β = 0.13, p < 0.01). The three predictors explained 85% of the variance of the 'perceived threat'.

6. Discussion

This survey tested the predictor structure of a model explaining reactions to the appraisal of risks resulting from ubiquitous ICT. The proposed model was based on implications of the protection motivation theory (Rogers, 1983) and on psychological risk research on the role of institutional trust and previous experiences.

In a first step, we were interested in factors predicting the two mediating processes of threat and coping appraisal. Evaluation with structural equation modeling supported the proposed effects of anticipated personal susceptibility and institutional trust on the perceived threat and coping efficacy. Thus, as the findings of other studies also suggested (Grothmann & Reusswig, 2006), the apprehension of personal harm enhanced the perceived threat resulting from ubiquitous ICT directly, and indirectly by increasing the negative affect. On the other hand, the presumption that other institutions, such as the government, consumer protection organizations, or producers, will ensure protection reduced the perceived threat indirectly by slightly decreasing the negative affect. This result is also in line with previous empirical findings (Grothmann & Reusswig, 2006; Kuttschreuter, 2006; Siegrist, 2000; Siegrist, et al., 2000). However, the strongest relationship emerged between the perceived threat and the negative affect with respect to ubiquitous ICT. The dominance of this relation is not surprising. Public knowledge on potential risks of ubiquitous ICT is little advanced, if not non-existent (Meier, 2005), and thus the topic was probably new to most of the interviewees. In cases where respondents lacked experience and knowledge, risk judgments tend to be based on affective sensations (Slovic, et al., 2004). The negative relation between previous ICT experiences and negative affect is in line with this as-

sumption, i.e., people experienced in the use of ICT were less frightened by the technological future than those without technological experiences. Furthermore, previous experiences were found to facilitate the appraised coping alternatives, thus supporting findings of Kuttschreuter and Gutteling (2004a) that experienced ICT users perceive their coping abilities to be higher than non-frequent users.

Other than hypothesized, the perceived benefits did not impede the perceived threat; rather, these two judgments seemed to be slightly positively related. A negative relationship between perceived benefits and risks has been repeatedly shown (Siegrist, Earle, Gutscher, & Keller, 2005; Siegrist, Keller, Kastenholz, Frey, & Wiek, 2007). However, in other studies, no association was found (Schütz & Wiedemann, 2008). Thus, the relationship between risks and benefits probably has to be investigated more deeply. Poortinga and Pigdeon (2006) argued that individuals cannot be characterized by either a positive attitude (high perceived benefits and low perceived risks) or a negative attitude (high perceived risks and low perceived benefits) towards genetically modified food. These authors proposed a third type with ambivalent attitudes, i.e., with both high-perceived benefits and risks. Thus, the positive correlation between perceived benefits and threat may indicate a widespread high ambivalence toward this new technology.

As a second step, we were interested in how the perceived threat and coping efficacies impacted potential responses. As proposed by the PMT (Rogers, 1983; Rogers & Prentice-Dunn, 1997) and found empirically (Floyd & Prentice-Dunn, 2000; Milne, et al., 2000), an increased appraised threat as well as increased coping efficacies intensified the protective responses, i.e., the intention to search for information on ubiquitous ICT as well as the intention to engage politically against the risks of ubiquitous ICT. However, the level of the perceived threat also enhanced the non-protective response. Thus, the critical predictor of the choice among protective or non-protective responses might be whether the person perceived high coping efficacies of the protective responses.

Finally, this study aimed at capturing the role of negative affect (the concept of fear in the original PMT) in more detail. This led to unexpected results; although the negative affect correlated positively with the appraised threat, these two components fundamentally differed in their impact on the response choice: The negative affect enhanced the non-protective response. However, unlike what Loewenstein et al. (2001) and Peters et al. (2006) had proposed, in this study, negative affect was not a motivator for the protective responses, but a handicap. This finding may be interpreted in the light of Leventhal's parallel process model (Leventhal, 1970; Leventhal, Diefenbach, & Leventhal, 1992), which assumes two different ways of processing threatening information. The first is a primarily cognitive process on an abstract, rational, and long-term level, while the second is a primarily emotional process on a more concrete, impulsive level. Whereas the cognitive process results in coping strategies to reduce the danger (similar to

the protective responses investigated), the second emotional process results in coping strategies to control the fear (thus the non-protective response). It might be that individuals experienced in ICT use judged the threats based on rather rational argumentations. As the strong relationship between previous ICT experiences and perceived coping efficacy indicate, this group of individuals may feel able to respond protectively. Their primary reaction might be the search for information, as this protective response relates much more strongly to the perceived threat than the intention to act politically. Conversely, individuals with only few previous ICT experiences may not have been well informed about the current technological trends and thus based their risk judgment on their affects. This group of individuals might lack the ability to react protectively and primarily search for control of affects by focusing on non-protective reactions. In line with these assumptions are the findings of Neitzke and colleagues that ICT experts rated risks of ubiquitous ICT to be higher than laypersons (Neitzke, et al., 2008).

Further experimental research on these relations, integrating Roger's PMT and Leventhal's parallel process model, would be promising, and first attempts in this direction have been made (Witte, 1998; Witte & Allen, 2000). Furthermore, group comparisons between experienced and non-experienced ICT users, conducted for example by Kuttschreuter and Gutteling (2004a), may reveal further insights.

As mentioned above, meta-studies on the PMT, e.g., by Milne et al. (2000), report only weak relations between the components of the perceived threat and the protective responses. This may be explained by the findings of the inhibitory effect of negative affect on the protective responses: If the cognitive components (such as severity), and the affective components (such as fear) of the threat appraisal are not explicitly distinguished, the two conflicting effects may compensate for one another and thus result in an insignificant overall effect.

6.1. Limitations

First, the topic of interest, namely the impacts of the diffusion of ubiquitous ICT, posed different challenges. The rather low public level of awareness rendered the introduction to the topic difficult within the limited setting of a structured questionnaire. A short introduction was chosen, describing the technological trends, combined with detailed questions on the concrete implication level. The innovative nature of this study legitimated this procedure. However, the possibility cannot be ruled out that the interviewees had different concrete scenarios or examples in mind while assessing the questions. For subsequent research, specifying the topic with a focus on concrete examples of applications would be preferable.

Second, this study should be understood as a snapshot of the current public position concerning future ubiquitous ICT. The results are based on cross-sectional data; the relations are therefore correlative and the assumed causality of a merely theoretical nature. It is self-evident that we

tried to base the causal model assumptions on previous theoretical and empirical findings. For instance, the assumed causal impact of the negative affect on the perceived threat has also previously been proposed and tested (Peters, Burraston, & Mertz, 2004; Peters, et al., 2006; Slovic, et al., 2002, 2004). The cross-sectional data basis, however, did not allow us to exclude the possibility of a reversed directional impact or even a bidirectional relationship. Thus, negative affect could be the emotional expression of a non-protective response (Wiebe & Korbel, 2003), i.e., caused through high perceived threat and low perceived coping efficacy. In this sense, the study disregarded the procedural character of a sequential appraisal process. The strengths and directions of the relations found have to be reassessed with a longitudinal research design, possibly in the form of a differentiated process model, which may account for different stages of problem awareness and decisions, such as that conducted by Block and Keller (1998) and Martens and Rost (1998), or in the form of a sequential process (e.g., that the coping appraisal only occurs if the threat is appraised as high), as proposed by Gardner and Stern (1996) and Witte (1998).

Third, the prospective character of this investigation only permitted the intentions to act protectively to be covered, and not the actions themselves (Webb & Sheeran, 2006).

Fourth, based on theoretical assumptions, the model tried to explain the major constructs of the threat appraisal process, and did so successfully, as the explained variances of the dependent variables showed. Due to the limited space in a questionnaire, a selection of constructs was necessary however. Thus, given the significant correlations between the error terms of the dependent variables, the existence of further common determinants, which were not included in the study, cannot be ruled out. Furthermore, the investigation of the perceived threat was narrowed to items assessing expectations similar to the 'vulnerability' of the original PMT, and refrained from assessing the 'severity'. Block and Keller (1998) found perceived 'vulnerability' to motivate individuals in an earlier stage of risk assessment, whereas perceived 'severity' only increased protective intentions for those already concerned with the risky topic. Thus, the assessment of the 'vulnerability' was more necessary to this study than that of the 'severity'. Furthermore, we were unable to investigate the influence resulting from external information sources; subsequent research should thus allow for predictors which characterize the message and source of such external information (e.g., the quality of arguments) and for underlying mediating or moderating processes (Das, deWit, & Stroebe, 2003; Meijnders, Midden, & Wilke, 2001a).

Fifth, as a consequence of the innovative character of this survey, there was no comparable research upon which to build, and thus no validated measurement instruments existed. The instrument used was developed for the purpose of this study; the content was derived from qualitative pre-studies. Nevertheless, the validity of the instrument used should be tested and the reliability could be improved. The rather poor reliability and low explained variances of the indicators of the 'non-protective response' may refer to a multidimensionality of this construct. The factorial overrepresentation by the indicator 'overstrain' means that the predictive struc-

ture found holds only for this non-protective response alternative, while the obtained results are inconclusive for the other captured variants such as denial or helplessness. Future research that uses models similar to ours should consider the components of the non-protective response as discrete constructs.

Sixth, similar to the research by Nerb et al. (1998) and proposed by Pfister and Böhm (2008), a differentiation of the construct 'negative affect' in emotions such as fear, anger, or sadness, as well as the differentiated investigation of their effects, could be useful.

Finally, no alternative models have been tested, a procedure recommended by MacCallum and Austin (2000) among others. The existence of further or other relations between the constructs, which may better represent the underlying data, cannot be ruled out.

6.2. Supporting protective behaviors

The overall purpose of this study was to gain insights into how people could be prepared for the incisive developments in the ICT domain, and on the extensive impacts of this trend on their daily environments. The 'classical way' is to foster protective, risk-mitigating behaviors indirectly by altering the appraised threat. This can be accomplished through risk communication campaigns, which inform people on aspects of potential threats (such as the severity or the personal susceptibility). However, based on the results, it must be noted that this approach only seems promising if some further aspects are taken into consideration. It has to be assumed that threatening information not only triggers cognitive appraisal processes but also, and at least to the same extent, negative affect, particularly fears (Peters, et al., 2006; Slovic, et al., 2004; Witte, 1998). This survey cannot exclusively answer the question as to what degree a possible intervention should actively provoke emotions. However, fear appeals, which enhance strong negative feelings, will certainly be counterproductive, as they may inhibit the formation of protective intentions and facilitate non-protective responses such as overstrain. On the other hand, moderate negative affect may be required to heuristically enhance the perceived threat and thus the protective response.

As noted by Bostrom and Fischhoff (2001) and confirmed by our findings, threat-enhancing communication only seems reasonable if it is combined with information on coping efficacy. Otherwise, the sensitizing efforts may result in non-protective responses. To facilitate protective coping behavior, ICT developers and regulators are asked to create basic conditions that prevent the discrimination and overstrain of different user groups as well as of non-users who are unwilling or unable to follow the technological trends. It is precisely these actors who may play a crucial role in people's responses to potential risks of future ICT. The findings show that institutional trust helps one to control the escalation of emotions. However, studies show that institutional trust is decreasing in society. Institutions that fail to communicate the risks may lead to a

loss of trust; and in the case of lacking institutional trust, risk communication may be counter-productive (Frewer, 2001, 2003; McCallum, Covello, & Peters, 1997).

Gardner & Stern (1996) argue that attempts to encourage protective actions should consider the individual psychological appraisal process, as well as allow for social, political, and other forces that affect individual behavior. Such a broad approach is needed to sensitize and help people cope with ongoing technological trends to enable them to proactively participate in designing the future daily life that we will live in.

Chapter 4:
A Dynamic Model of Individual Information System Security Threat Control

Parts of this chapter have been prepared for submission as:
Moser, S., Groesser, S.N., & Bruppacher, S.E. (Manuscript prepared for submission). Managing Security Threats to Information Systems: A Dynamic Model of Controlling Individual Threats.

Abstract

Considerable damage to information systems (IS) results from security incidents provoked by careless or naïve end-user behavior. For a better understanding of this phenomenon, a model is needed which explains the emergence or absence of end-user IS security behavior over time. A first such process model is the technology threat avoidance theory (TTAT), which adopts a control theoretical approach to explain individual IS security behavior. The present study extends the general dynamic model propositions of the TTAT by formalizing and testing a mathematical model that allows for simulating the evolution of individual IS security behavior over time. The model presented supplements the TTAT with elements from unidirectional, and control-theoretical approaches on risk perception and coping behavior. The ability of the model to reproduce behavior similar to that assumed by theory-driven propositions was tested and its behavior space was explored by manipulating exogenous factors. As expected, the simulations revealed that the tolerated threat threshold determined the resulting level of individual IS security behavior. Surprisingly, providing more information about risks turned out to be counterproductive in the case of low perceived coping efficacy. Furthermore, efforts to enhance perceived coping efficacy were only successful in increasing individual IS security behavior when combined with increases in the perceived overall threat and decreases in the tolerated threat threshold. In conclusion, the limitations of the model as well as implications for further research and practice are discussed.

Keywords: Process Theory, Control Theory, System Modeling, Protection Motivation Theory, Risk Perception, Threat Appraisal, Information System Security Behavior

1. Introduction

People who at least occasionally use information and communication technologies (ICT) are increasingly confronted with security issues. These may occur in the form of reports on destructive computer viruses, a friend's unfortunate experience opening a contaminated e-mail, or warnings from one's own computer that the security software will expire soon. People respond to this risk information by adopting more or less effective coping strategies, such as regular changes of passwords, updates of security software, frequent data backups, avoidance of suspicious Internet contents, or cancellation of the annoying automatic virus scanning (Whitman, 2003; Workman, et al., 2008).

End-users' responses in managing ICT threats are an essential determinant of the annual damage to individuals and society caused by information security incidents. Threats to the information system (IS) caused at least partially by end-user behavior include unauthorized interception or modification of data, exposure of data to unauthorized individuals as well as the destruction of hardware, software, and information for which effective protective measures would exist (Workman, 2007). It is estimated that up to 80% of all security breaches in organizations may be the result of social engineering[3] and inappropriate end-user behavior (Leach, 2003). Therefore, end-user security behavior has been considered to be the weakest link in the IS security system (Rhee, Kim, & Ryu, 2009; Sasse, et al., 2001). This is because a completely automated protection system is often unfeasible for financial, situational, ethical, or technical reasons (Post & Kagan, 2007; Rhee, et al., 2009; Workman, et al., 2008).

Thus, the compliance of users with individual security management is required to achieve a high IS security level. Up to now, however, research has treated the IS security issue as merely a technical problem (Sasse, et al., 2001). It is only recently that calls to consider the human dimension of IS security risks have been addressed by researchers through empirical work on psychological predictors of individual IS security behavior (e.g., by Ng, Kankanhalli, & Xu, 2009; Rhee, et al., 2009; Workman, 2007; Workman, et al., 2008). Most of these studies have followed conventional unidirectional approaches with cross-sectional designs. The underlying models were recursive, i.e., they accounted for causation between variables in only one direction. Such one-way models neglect potential feedback processes that may occur when behavior is investigated over time. Clearly, there is a need for more comprehensive models capable of explaining individual IS security behavior over time. Liang and Xue (2009) made a first step in this direction with their 'technology threat avoidance theory' (TTAT), which understands individual IS security behavior (termed threat avoidance behavior by these authors) as part of a dynamic process. By adapting

[3] In the context of IS security, this term implies the intended manipulation of people in order to bypass technical safeguards, e.g., by persuading users or by exploiting their naivety.

cybernetic control theory (Ashby, 1956; Wiener, 1948), the TTAT integrates propositions of the protection motivation theory (PMT) of Rogers (1975, 1983; 1997) in a feedback model. The model is regulated by an internal anti-goal concept and reacts to environmental changes, such as the emergence of destructive information technologies.

In contrast to common unidirectional approaches, cybernetic control models step beyond mere one-way relationships. Human behavior is not regarded as the dependent variable which is to be explained, but as being endogenously embedded in a self-regulating system, which allows for dynamic interactions between internal model elements and environmental influences (Edwards, 1992; Richardson, 1991; Vancouver, et al., 2005). Unfortunately, Liang and Xue's (2009) description of the TTAT remains on a verbal level only. A purely textual description of complex dynamic feedback processes carries with it the potential of inconsistencies, ambiguity, and misspecifications (Sterman, 2001; Vancouver, 2005), which we think are relevant shortcomings of the TTAT. It is the aim of the present study to address the inconsistencies and imprecision of the TTAT by developing a computer-based simulation model of individual threat control. This model builds on the process-oriented assumptions of the TTAT which have been enhanced by detailing them theoretically and by formalizing them into a computer-based, mathematical simulation model. Computational simulation models can be validated by comparing alternative model structures, and by testing the ability of the model to replicate theoretically derived assumptions on behavior (Vancouver, et al., 2005). Thus, we addressed the following questions:

- First, which dynamic core structure best fits the theoretical considerations?
- Second, is our proposed model able to replicate theoretical propositions regarding changes in individual IS security behavior?

Furthermore, using the validated model, we were interested in exploring how individual IS security behavior could be enhanced or supported under consideration of varying conditions. Thus, third, we ask:

- How can a high level of individual IS security behavior be achieved?

In the following theoretical section, the theoretical model structure proposed by the TTAT, as well as an alternative structure, are introduced. It is perhaps worthwhile mentioning here that the test of our first research question revealed that the model structure proposed by the TTAT was less convincing than the alternative structure (cf. the findings in section 4.1). Therefore, based on the alternative structure, a new model was proposed whose elements are theoretically detailed in the subsequent section. Next, propositions on changes in individual IS security behavior are theoretically derived, which our model simulation should be able to replicate. Follow-

ing the theoretical part, the modeling method is introduced. The subsequent result section starts with the presentation of the mathematical model, followed by the test of the model alternatives, the replication of the behavior propositions, and ends with explorative simulations on potential interventions. In conclusion, we discuss our findings, describe the limits of our undertaking, and present implications for further research and practice.

2. Control-theoretical approaches to individual security behavior

Control theories, also called self-regulating theories, assume intentional behavior to stand in a reciprocal relationship with the perception of present environmental conditions (Ashby, 1956; Carver & Scheier, 1982; Edwards, 1992; Wiener, 1948). The basic structure of control-theoretical models is a goal-seeking feedback loop, i.e., a closed chain of causally linked elements which compares an internal reference value, i.e., a desired end state or goal, with the perceived state of the current external environmental conditions. A discrepancy between these two states activates corrective behaviors, aimed at reducing the discrepancy. The adapted environmental state is reappraised and the discrepancy thus reduced (Levine, et al., 1992; Sterman, 2000). In analogy to a thermostat, a goal-seeking feedback structure tries to regulate the perceived current state to the reference value, which exerts a directive function on the behavior (Carver and Scheier 1982; Elliot 2006). If the perceived current state is equal to the reference value, the system is stable and no corrective actions occur. An external disturbance, however, may create a new discrepancy between the perceived state and the reference value. Then, the goal-seeking process is re-triggered; the system seeks to re-find a stable state by re-activating the corrective behavior.

In addition to the goal-seeking feedback loop, Carver (2006) describes a second type of feedback structure: a goal-avoiding feedback loop. In this structure, the reference value represents an undesired end state, i.e., an anti-goal, and the corrective behavior acts in order to increase the discrepancy between the perceived state and the reference value. The TTAT (Liang & Xue, 2009), which will be presented in the next section, is based on this goal-avoiding structure. Since we challenge the usefulness of a goal-avoiding structure with regard to individual IS security behavior, we introduce then two theories based on the original goal-seeking structure. The first in section 2.2 is the perceptual control theory (PCT) (Powers, 1973, 1990), a basic control-theoretical application to individual behavior. The second, in section 2.3, is the risk homeostasis theory (RHT) (Wilde, 1982b, 1998), an application of the goal-seeking structure to individual risk perception. For our model of individual threat control, presented in section 2.4, we have integrated elements of these three theories. To conclude the theoretical section, we outline in section 2.5 propositions on changes in individual IS security behavior, which we used for validating the model later on.

2.1. Technology threat avoidance theory (TTAT)

The technology threat avoidance theory (TTAT) of Liang and Xue (2009) assumes individual IS security behavior to be based on a goal-avoiding feedback loop[4], as shown in the model in Figure 4.1. The TTAT stipulates that a threat-avoiding process is triggered by an external disturbance, such as the emergence of destructive information technologies, which is perceived by the users. This perception is compared with the anti-goal of 'being harmed by malicious IT'. If the resulting perceived discrepancy between the perception of the situation and the anti-goal is lower than a tolerable threshold, a threat is perceived. Thus, the perceived threat is inversely proportional to the perceived discrepancy between the current state and the anti-goal; the smaller the discrepancy, the higher the perceived threat.

Summarizing unidirectional models, such as the protection motivation theory (Rogers, 1975, 1983), the TTAT posits that this first appraisal of the threat is followed by the coping appraisal, which assesses different safeguarding measures regarding their efficacy. In the case that the threat may be perceived as manageable, the individual engages in problem-focused coping, for instance by increasing his or her IS security behavior. Increased security efforts reduce the perceived threat and as a consequence, the difference between the perceived threat and the anti-goal increases (cf. path 1 in Figure 4.1). Alternatively, if the potential safeguarding measures are perceived as impracticable, the individual engages in emotion-focused coping (path 2). Thus, the objective threat is not changed, but the subjective perception thereof, for instance, by minimizing its negative consequences (Beaudry & Pinsonneault, 2005; Liang & Xue, 2009). In both cases, the feedback structure controls the perceived threat by increasing the distance to the anti-goal.

However, the TTAT contains several unspecific or inconsistent elements regarding its control-theoretical foundation: First, the theory fails to theoretically derive its reference value, i.e., the anti-goal. Second, appraisals of threats and coping options are cognitive processes (Rogers & Prentice-Dunn, 1997). Intentional cognitive processes are typically linked to goal-seeking behavior. Goal-avoiding reactions, however, have been described as first instinctive responses to

[4] The authors of the TTAT use the expressions 'goal-avoiding' or 'positive' feedback loop synonymously; however, they fail to specify their understanding of a positive feedback loop. Richardson (1991) defines a positive loop as reinforcing or amplifying a change in any of its elements, whereas a negative or goal-seeking feedback loop diminishes or counteracts a change in its elements. Thus, in the former type of loop, an increase in a variable, e.g., an increase in destructive ICT enhancing the perceived threat, feeds around the loop and tends to cause the original variable to increase even further. Conceptually, the polarity of a loop can be determined by the polarity of the product of its causal links; a positive loop contains an even number of negative links, and a negative loop an odd number of negative links (Levine, et al., 1992; Richardson, 1991). A self-regulating structure which increases the perceived threat exponentially certainly does not correspond to the model which the authors of the TTAT intended to describe. Also, an examination of the loops' polarity (cf. Figure 4.1) reveals odd numbers of negative links. Thus, the expression 'positive feedback loop' in relation to the model structure of the TTAT is incorrect and will be avoided within this chapter.

stimuli, unmediated by any higher-order cognitive processes (Elliot and Covington 2001) and preferences for approaching or avoiding behavior have been attributed to individual differences in personality (Carver and White 1994; Sherman, Mann et al. 2006). Thus, the suitability of a goal-avoiding structure in modeling a cognitive risk theory needs to be questioned.

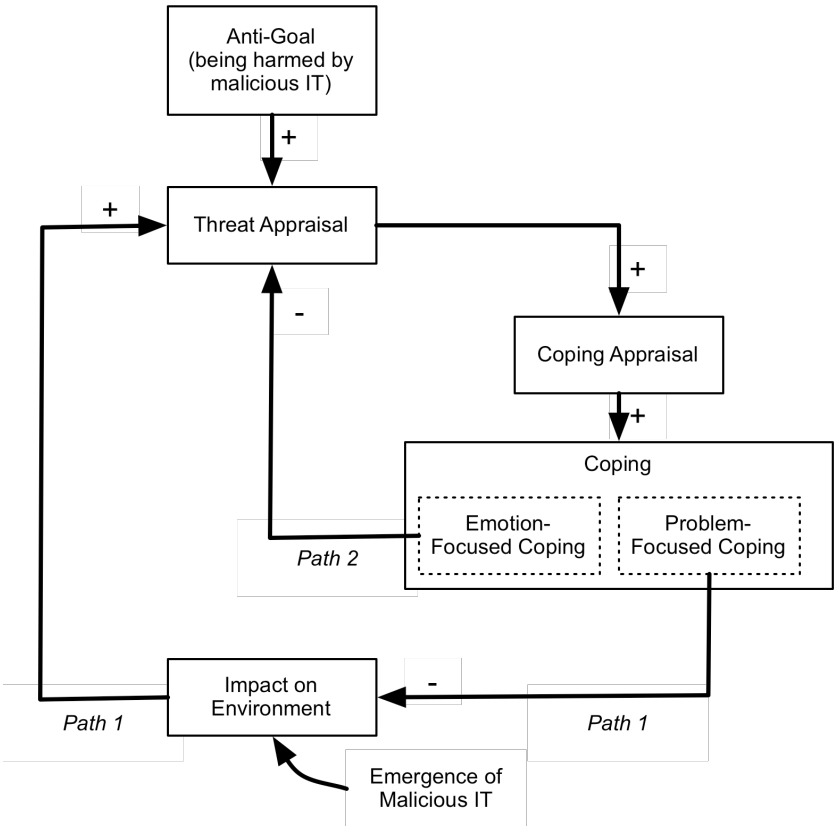


Figure 4.1. Goal-avoiding feedback structure of the TTAT (adapted from Liang & Xue, 2009).

Third, in the goal-seeking structure, the reference value defines the direction of the corrective behavior, i.e., the behavior tries to approach the perception to the reference value until the former equals the latter. Conversely, goal-avoiding behavior is without affirmative direction; behaviors away from the anti-goal in the form of decrease are as good as those in the form of increase. Carver and colleagues posited that every goal-avoiding behavior must at one point pass into a goal-seeking one (Carver and Scheier 1990; Carver 2006; Rassmussen, Wrosch et al. 2006); otherwise, the avoiding behavior continues infinitely. The TTAT makes no statements about the lacking direction. Probably, the authors assume that the direction of the behavior is implicitly given, i.e., that the distance between the current situation and the anti-goal will be enlarged by reducing the danger, rather than by increasing it above the anti-goal. In order to address the problem of the infinite behavior, the TTAT introduced a tolerance level, which represents the 'minimum discrepancy between the undesired end state (attacked by malicious IT) and the current state that users are able to tolerate' (Liang and Xue 2009, p.84).

These inconsistencies of the TTAT motivated us to search for alternative model structures, which adopt the original control theoretical structure – the goal-seeking feedback loop. Two such frameworks, the perceptual control theory and the risk compensation theory, are presented in the following.

2.2. Perceptual control theory (PCT)

Based on the concept of feedback, the perceptual control theory (PCT) of Powers (1973, 1990) depicts a model of individual behavior in the form of goal-seeking feedback loops, on different hierarchical levels, as shown in Figure 4.2. The hierarchical levels are descending in abstractness, which is matched by the different feedback loops. The output of each loop on a hierarchical level constitutes the reference value for the loop on the subordinate, more concrete level, with behavior in the form of physical movement as the output of the lowermost level.

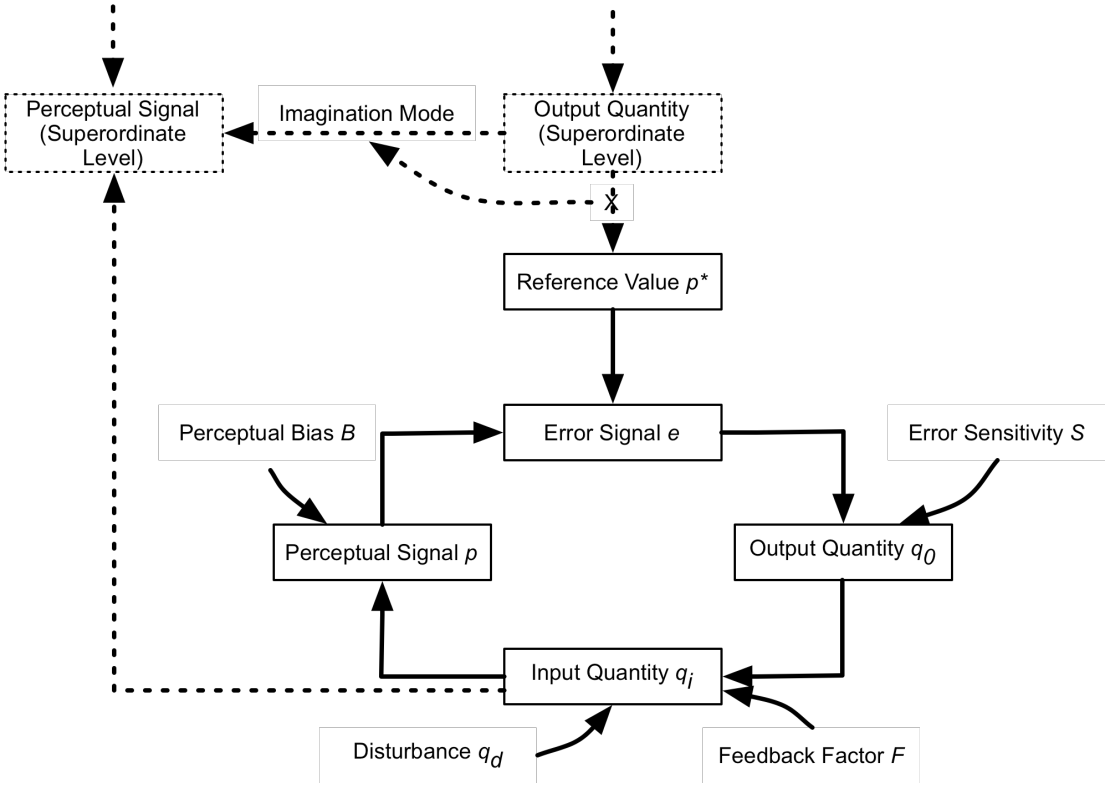


Figure 4.2. Goal-seeking feedback structure of the PCT (adapted from Powers, 1973; 1990)

PCT has been called a groundbreaking application of control theory in the social sciences, since it provides one of the rare mathematical operationalizations for the goal-seeking feedback structure of human behavior, while the vast majority of the control theoretical approaches remain on a verbal level (Richardson, 1991; Vancouver, 2005). The mathematical formulations of the relationships among the feedback model's components are the following (cf Figure 4.2):

The error signal e is the result of the comparison of the reference value p^* with the perceptual signal p (Eq. 1). If the error signal is multiplied with an error sensitivity factor S, the output quantity q_o is the result (Eq. 2):

$$e = p^* - p \quad \text{(Eq. 1)}$$

$$q_o = S^* e \quad \text{(Eq. 2)}$$

The output quantity, multiplied by a feedback factor F and added to a disturbance q_d, weighted with the Factor D, results in the input quantity q_i (Eq. 3):

$$q_i = F^* q_o + D^* q_d \quad \text{(Eq. 3)}$$

Furthermore, it can be assumed that the perceptual signal p is a biased version of the input quantity, represented by a bias factor B (Eq. 4):

$$p = B^* q_i \quad \text{(Eq. 4)}$$

Powers' assumption of a goal hierarchy was adapted by Carver and colleagues (Carver & Scheier, 1982, 1990; Powers, 1973; Rassmussen, Wrosch, Scheier, & Carver, 2006; Scheier & Carver, 2003). Following these authors, on the lowermost level, the feedback structure is guided by motor control goals, which create physical movements. The motor control goals result from the superior 'program' level containing action or 'do' goals. The action goals emerge, for their part, from values or principles, so-called 'be' goals, which are influenced by the uppermost abstraction level, the 'ideal self' or system concept level (Carver, 2006; Rassmussen, et al., 2006; Scheier & Carver, 2003). The goal's abstraction level reflects its stability and importance. Goals on a higher level are more tied to the sense of self and thus more resistant to change (Carver, 2006).
The PCT describes behavior as a reaction to perceived changes in the real external environment. Security behavior, however, is preventive behavior. This means that an individual has to anticipate potential undesired external changes, for example IS incidents, and prevent them before they effectively manifest themselves. This phenomenon is similar to the 'imagination mode' the PCT describes. This mode is either used to test control actions without carrying them out, or to supply missing perception (Powers, 1973). As shown in Figure 4.2, this is done by temporarily switching the connection between the output of a subsystem of the goal hierarchy and the reference signal of a lower system, so that the output enters the input of the same system (Powers, 1973, 1991).

2.3. Risk homeostasis theory (RHT)

The risk homeostasis theory (RHT), sometimes also referred to as risk compensation theory (Simonet & Wilde, 1997; Wilde, 1982a, 1982b, 1998), originates in research on traffic safety. This approach emerged independently of the PCT and prior to the TTAT. Conversely to the TTAT, the RHT assumes a goal seeking-feedback structure with the 'target level of risk' serving as the reference value. The target risk level is defined as the amount of risk an individual is willing to take (Wilde, 1998). This concept thus shows a strong analogy to the 'tolerance level' included within the TTAT (Liang & Xue, 2009).

Following the argumentation of the RHT, the target risk level is not minimized, but optimized (Wilde, 1998). Only in the case of a user fully resigning from the benefits of a risky behavior may the tolerated risk level be zero. As long as a certain behavior (e.g., using the Internet) results in some conveniences, the individual balances the risks of the behavior against the benefits in order to find an acceptable risk level.

According to the RHT, individuals seek to maintain the perceptual signal (named 'perceived level of risk' in the RHT) on the acceptable level specified by the reference value (Wilde 1982b; Wilde 1998). In addition, the RHT infers that if the perceived level of risk falls below the target risk level the individual compensates for the error signal by adopting a riskier behavior style (hence the name risk compensation). Thus, in contrast to the TTAT, the RHT explains not only security behavior, but also risky behavior. Risk compensation may be provoked by an implementation of structural or technological safeguarding measures, i.e., a decrease in the perceived level of risk due to external disturbances. As examples, the author of the RHT mentions evidence that safety measures, such as the seatbelt laws or the use of airbags and anti-block brakes, did not result in an overall decrease in the traffic death rate per inhabitant. Due to these structural safety measures, fewer car drivers died, but, as they compensated with a riskier driving style, there were more victims among cyclists and pedestrians (Simonet & Wilde, 1997; Wilde, 1982b).

There is a shared acceptance of the phenomenon of risk compensation (Trimpop, 1996). Other aspects of the RHT, however, have been criticized; for example, the unrestricted system boundaries, which make it impossible to falsify the model empirically (Evans, 1986; Slovic & Fischhoff, 1982; Thompson, et al., 2001), and the mixing of individual and societal model levels, which blur the concepts (Cole & Withey, 1982; Trimpop, 1996). Of particular importance to the present study are criticisms regarding the concept of the target risk level: the RHT simplifies this trade-off to four utility factors, namely, the expected benefits of the risky behavior alternatives, the expected costs of security behavior alternatives, the expected costs of risky behavior, and the expected benefits of security behavior alternatives. Consequently, the RHT sees extrinsic motivators in the form of monetary incentives and punishment as the only sustainable way to change security behavior (Wilde, 1982b, 1998). From a psychological perspective, this argumentation is

strongly reduced and neglects intrinsic motivators (Trimpop, 1996). Moreover, it renders the model behavior unstable, as incentives may vary from one moment to the next (Slovic & Fischhoff, 1982). In sum, the conceptualization of the RHT, namely, the reference value as target risk level, is an attractive alternative to the reference value in the form of an anti-goal as offered by the TTAT. However, to overcome the criticisms mentioned above, the concept of target risk has to be elucidated further.

In conclusion, the three control-theoretical approaches outlined above – TTAT, PCT, and RHT – provide structural elements to explain individual IS security behavior. However, particularly the two approaches involving risk perception, TTAT and RHT, contain several inconsistencies that could be reduced by combining the approaches. This is done in the next section, where we introduce the elements and structure of the model of individual threat control we propose.

2.4. Theoretical specification of the model of individual threat control

The proposed model of individual threat control consists of two goal-seeking feedback loops, which correspond to the two paths of the TTAT. The first loop about threat control, depicted in Figure 4.3, adapts the loop structure of the PCT. As shown in Figure 4.4 , this first loop is supplemented with a second loop, which adjusts the reference value. The elements of the two loops are detailed in the following.

Tolerated threat threshold: Specifying the reference value

The goal-seeking feedback structure implies a reference value in the form of a desired state or goal. As shown in Figure 4.3, we adapted the reference value of the RHT (Wilde, 1982b, 1998) by assuming that an individual adjusts his or her IS security behavior to the individual 'tolerated threat threshold', i.e., the level of risk an individual is willing to sustain. Contrary to the RHT, we do not assume that this tolerated threat threshold is only based on behavioral utility factors. Rather, we follow the propositions of the goal hierarchy (Carver & Scheier, 1990; Powers, 1973; Scheier & Carver, 2003) and suppose that the tolerated threat threshold emerges from the output of the superior hierarchical goal level. Individual IS security behavior may be ascribed to the program level. Hence, the tolerated threat threshold is affected by the output of the superior principle level, i.e., it consists of a trade-off between IS security principles and principles competing them. IS security principles may, for instance, be the awareness and valued importance of the integrity, confidentiality and availability of data, responsibility for one's own actions, efficient use of electronic communication, privacy, or the strategic risk management principles of an organization (Carver & Scheier, 1990; Drevin, Kruger, & Steyn, 2007; Smith, 1989; Stewart, 2004), but also social norms (Herath & Rao, 2009) or personal norms (Loroz & Lichtenstein,

2004). It is known that increased IS security may interfere with competing principles, such as job responsibilities or the satisfactory completion of work tasks on time, as safeguarding measures may lead to restricted data access and lower productivity (Post & Kagan, 2007).

Furthermore, highly valued leisure time principles, such as the importance attributed to the sharing of music files via the Internet, may compete with security principles. Thus, on the level of the reference value, a potential intervention to enhance security behavior seems to lie in the strengthening of supporting security principles and smoothing out competing principles in order to reach a lower tolerated threat threshold.

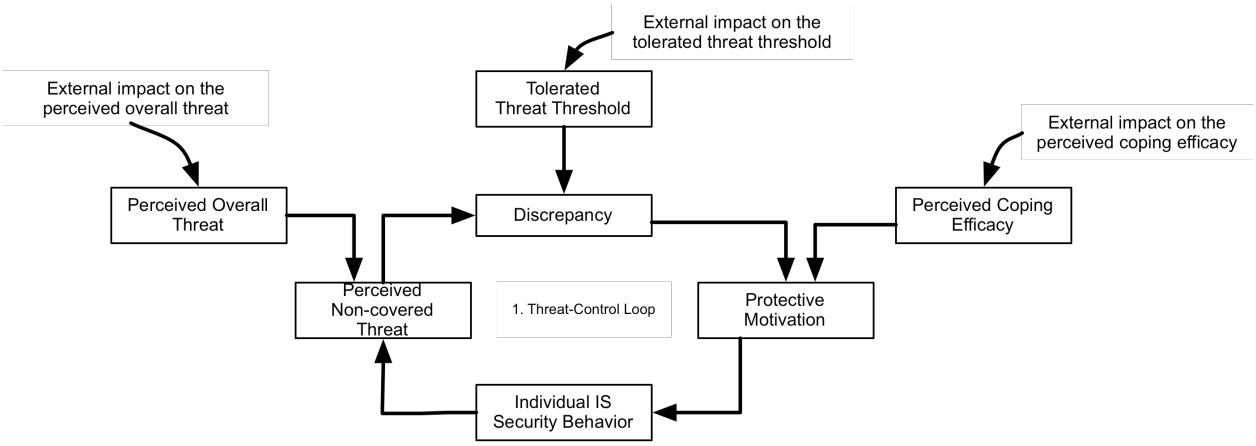


Figure 4.3. Depiction of the threat-control loop of the proposed model of threat control

Threat appraisal: Specifying the left-hand side of the threat-control loop

The left-hand side of Power's model (cp. Figure 4.2) describes the causal chain from the input quantity via the perceptual signal to the error signal. The aim of this section is to adapt this structure to the model of threat control.

First, we specified the input quantity. Assuming individual IS security behavior to be a preventive behavior, an individual may not expect to change real environmental states with security measures; rather, the security behavior is thought to be successful when the status quo remains unchanged (i.e., no virus infection). Thus, there are no changing environmental states that feed back to the perceptual signal. The individual has to replace this missing information by assuming an effect directly from the executed security measures (cf. section 2.2 about the imagination mode of Powers, 1973; 1991). Thus, we suppose, as depicted in Figure 4.3, that the current level of performed 'individual IS security behavior' constitutes the input quantity. By 'individual IS security behavior' we refer to the number of accomplished security measures and omitted risky behaviors averaged over a certain period of time (e.g., per month). IS security is not achieved by a single action, such as the one-time completion of hazard insurance; rather, it requires a set of

repeated actions and omissions, e.g., the regular updating and changing of passwords. Therefore, individual IS security behavior is best represented as an average of the protective behavior level.
Second, we assume that, based on the performed security measures, the individual estimates the 'perceived non-covered threat' analogically to the perceptual signal of the PCT. The effect from performed security measures on the reappraisal of the threat level has only rarely been empirically investigated (and only in the context of health threats). However, these results indicate that previous protective behavior reduced the level of the perceived threat and that, under consideration of the precautionary measures undertaken, susceptibility judgments were relatively accurate (Brewer, Weinstein, Cuite, & Herrington, 2004; Gerrard, Gibbons, & Bushman, 1996; Renner, Schüz, & Sniehotta, 2008). Thus, we suppose that the higher the individual IS security behavior, the lower the perceived non-covered threat.
Third, following the model structure of the PCT, we assume, as shown in Figure 4.3, that the perceived non-covered threat is compared to the tolerated threat threshold in order to ascertain a possible 'discrepancy'.
Fourth, the perception of the current threat is not solely based on previous security measures, but also on an estimation of the overall exposure. This relationship has been the main issue of many unidirectional theoretical frameworks, such as the protection motivation theory PMT (Rogers, 1975, 1983) or the extended parallel process model EPPM (Witte, 1994; Witte & Allen, 2000). The common notion of these frameworks is the assumption that 'external impacts on the perceived overall threat' in the form of informative communication about, for example, the high severity and likelihood of occurrence (vulnerability) of a threat, mediated by the threat appraisal process, impact on the motivation to protect against the threats (Milne, et al., 2000; Neuwirth, Dunwoody, & Griffin, 2000; Rogers, 1975, 1983; Rogers & Prentice-Dunn, 1997).
The notion that external risk messages act as external disturbances and thus trigger the threat appraisal process has been adopted by the TTAT (Liang & Xue, 2009). However, the TTAT remains rather unspecific about the exact underlying model structure. Furthermore, we assume that the PCT structure has to be adapted in this point in order to explain preventive behavior; the external disturbance in this case has to affect the perceptual signal rather than the input quantity. Thus, we suppose that external risk messages impact on the estimation of an 'overall threat', which, in turn, increases the perceived non-covered threat. In contrast to the TTAT we therefore distinguish between three concepts relevant to the threat appraisal: The 'perceived overall threat' reflects the perceived general exposure. The 'perceived non-covered threat' compares this general risk judgment with the individual situation under consideration of the security measures previously undertaken. Finally, the 'discrepancy' weighs the perceived threat to individual principles and values.

Coping appraisal: Differentiating the right-hand side of the threat-control feedback loop

A perceived discrepancy between the perceived non-covered threat and the tolerated threat threshold motivates individuals to react. The PCT proposes that the effect of the discrepancy on the output quantity depends on a further element: the error sensitivity factor. In a similar way, unidirectional approaches, such as the protection motivation theory, assume that, supplementary to the perceived threat, a second appraisal process impacts on the protective motivation. In this so-called 'coping appraisal', the individual evaluates potential safeguarding measures for their effectiveness, self-efficacy, and costs, resulting in a judgment about the perceived coping efficacy (Liang & Xue, 2009; Rogers, 1975, 1983). Previous research has found that higher levels in the components of the coping appraisal are related to higher levels of risk-mitigating behavior in general (Floyd & Prentice-Dunn, 2000; Milne, et al., 2000; Rogers & Prentice-Dunn, 1997) and of individual IS security behavior in particular (Ng, et al., 2009; Rhee, et al., 2009; Workman, et al., 2008). Thus, communication or policies fostering coping options, for example in the form of IT training, are expected to increase the 'perceived coping efficacy'. Together with the perceived discrepancy, perceived coping efficacy impacts on protective motivation, as depicted in Figure 4.3. The protective motivation corresponds to the output quantity of the PCT and, in turn, changes the input quantity, i.e., the individual IS security behavior.

From a control-theoretical perspective, the perceived coping efficacy may represent an expectancy assessment about the achievement of the goal. Carver and colleagues propose that discrepancy-reducing behavior depends on such an expectancy assessment, which is separate and distinct from the discrepancy-reducing process itself (Carver & Scheier, 1990; Rassmussen, et al., 2006). These authors define goal achievement expectancies as the expected rate of progress toward the goal. Thus, the expectation of how fast the discrepancy between goal and perceptual signal can be reduced determines how much effort is invested in the behavior to reduce the discrepancy.

Emotion-focused reactions as goal adjustment: Expanding the model with a second feedback loop

The final question is what happens when coping is perceived to be inefficient in reducing the discrepancy between the perceived non-covered threat and the tolerated threat threshold. Following unidirectional theoretical propositions, the individual builds a 'defensive motivation', which leads to an emotion-focused reaction (Rogers & Prentice-Dunn, 1997; Witte, 1998). This means that the stress caused by the threat is reduced by negating the threat, by denying it, by avoiding thinking about it, or by wishful thinking (Liang & Xue, 2009). Empirical studies have shown that the stronger the perceived threat and the weaker the perceived coping efficacy, the larger is this emotion-focused response (Rippetoe & Rogers, 1987; Witte & Allen, 2000).

From a process theoretical point of view, a perceived low coping efficacy means that the discrepancy is not expected to be reduced within a foreseeable timeframe. This provokes stress with negative consequences for individual well-being. Efforts and energy are wasted on unattainable goals and are thus inaccessible for the attainment of other goals (Carver & Scheier, 1990; Rassmussen, et al., 2006; Wrosch, Miller, Scheier, & Brun de Pontet, 2007; Wrosch, Scheier, Carver, & Schulz, 2003). In this case, an adaptive reaction is to adjust the goal to conform with perceptions (Edwards, 1992). The individual thus has to disengage from the previous goal by assigning it lower priority, which opens the possibility to re-engage in alternative or less ambitious, attainable goals (Carver & Scheier, 1990; Rassmussen, et al., 2006; Scheier & Carver, 2003). Therefore, the individual has to shift his or her awareness to the next higher hierarchical goal level (Carey, 2008). Only an adjustment of the original goal can prevent repeated goal failure and the associated negative emotions (Edwards, 1992; Rassmussen, et al., 2006; Wiebe & Korbel, 2003). Repeated goal failure, with an inability to adjust a goal may provoke feelings of helplessness, hopelessness and depression, and may even end in suicide (Scheier & Carver, 2003).

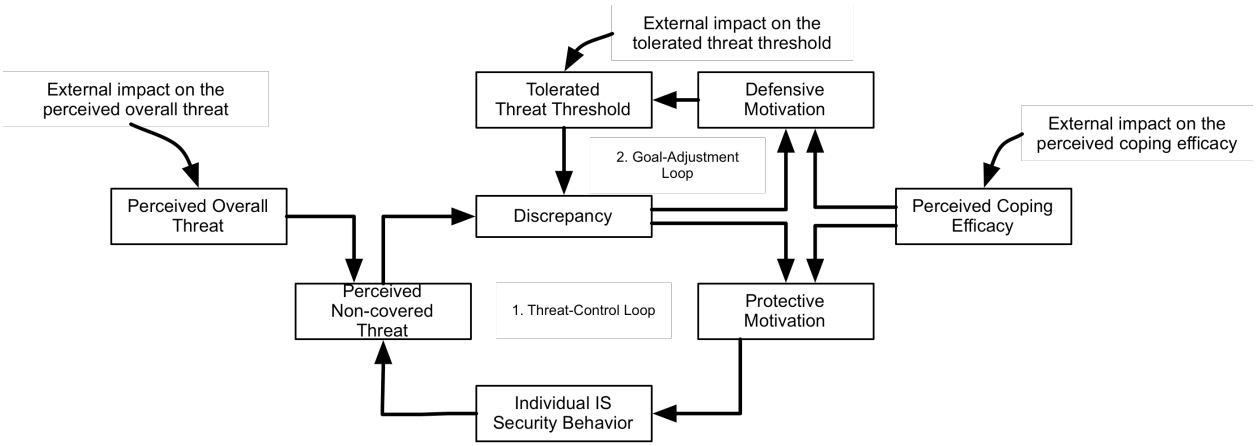


Figure 4.4. Depiction of the goal-adjustment loop of the proposed model of threat control

The process of goal adjustment can be formalized by the structure of 'drifting goals' (Levine & Doyle, 2002; Wolstenholme, 2003). This structure supplements the classical goal-seeking feedback loop with a second loop from the error signal to the reference value, as shown in Figure 4.4. Thus, we assume that the emotion-focused reaction works via the reference value. This assumption is contrary to the TTAT, which proposes that the emotion-focused reaction impacts directly on the error signal.

2.5. Propositions regarding individual IS security behavior changes

As described above, the theoretical assumptions and empirical indications offered directions for the formulation of the elements and structure of the model of individual threat control. Moreover, they allow for extracting propositions on behavior changes under different preconditions. Such propositions on individual IS security behavior will be detailed in the following. These propositions are used to validate the assumed model by testing whether the model produces behaviors as theoretically expected.

Following the notions of the RHT (Wilde 1982b; Wilde 1998), individuals seek to maintain the perceptual signal, in our case the perceived non-covered threat, on an acceptable level specified by the reference value, i.e., the tolerated threat threshold. This is done by changing the security behavior level. Thus:

P1: A low threshold of tolerated threat results in a higher individual IS security behavior than a high threshold of tolerated threat.

Perceived threat and perceived coping efficacy impact on risk-mitigating behavior (Floyd & Prentice-Dunn, 2000; Liang & Xue, 2009; Milne, et al., 2000; Ng, et al., 2009; Rhee, et al., 2009; Rogers, 1975, 1983; Witte & Allen, 2000; Workman, 2007; Workman, et al., 2008). Following these findings, we propose that:

P2: A high level of perceived overall threat provokes a higher level of individual IS security behavior than a low level of perceived overall threat

and

P3: A high level of perceived coping efficacy results in higher level of individual IS security behavior than a low level of perceived coping efficacy.

Empirically, an interaction effect between threat and coping appraisal has been found. In the case of high perceived coping efficacy, higher levels of the threat appraisal predictors resulted in stronger protective responses than under low perceived threat (Cismaru & Lavack, 2007; Eagly & Chaiken, 1993; Rogers & Prentice-Dunn, 1997; Witte & Allen, 2000). Furthermore, previous research has revealed that the level of the protective response was similar under conditions of low threat – high coping, and high threat – low coping. The lowest protective response emerged, however, in a low threat – low coping condition (Witte & Allen, 2000). Thus:

P4: The resulting level of individual IS security behavior should be highest under the condition in which a high level of perceived overall threat is combined with a high level of perceived coping efficacy and lowest under the condition in which a low level of perceived overall threat is combined with a low level of perceived coping efficacy.

However, following the assumptions of the RHT about risk-compensating behavior, the above-listed propositions are only valid if the tolerated threat threshold is lower than the perceived overall threat. Otherwise, the perceived negative discrepancy will be compensated for by lowering the security measures:

P5a: The perception of an overall threat level exceeding the tolerated threat threshold provokes an increase in the level of the individual IS security behavior, i.e., a threat-controlling behavior.

P5b: The perception of an overall threat level lower than the tolerated threat threshold provokes a decrease of the level of individual IS security, i.e., a threat-compensating behavior.

Further, we address the defensive motivation. As mentioned above, unidirectional empirical findings suggest that the stronger the perceived threat and the weaker the perceived coping efficacy, the stronger the defensive motivation and the emotion-focused reaction, respectively (Rippetoe & Rogers, 1987; Rogers & Prentice-Dunn, 1997; Witte, 1994, 1998; Witte & Allen, 2000). Thus, transferring this to the control-theoretical model, we propose that:

P6: The resulting threshold of tolerated threat should be highest under the condition in which a high level of perceived overall threat is combined with a low level of perceived coping efficacy, and lowest under the condition in which a low level of perceived overall threat is combined with a high level of perceived coping efficacy.

3. Modeling with the system dynamics methodology

We chose System Dynamics (SD) methodology (Forrester, 1961; Sterman, 2000) to operationalize our model of individual threat control, using Vensim software. System Dynamics (SD) originates from nonlinear feedback control theory and is therefore well suited to the development of our formal model. The methodology has been successfully applied to issues such as corporate development (Forrester, 1961), urban evolution (Forrester, 1969), diffusion of innovations (Repenning, 2002), environmental issues (Ford, 1990, 1999), changes in social systems such as schools (Hirsch, Levine, & Miller, 2007) or public health systems (Homer & Hirsch, 2006). It has

also been used in psychological research to model generic structures of social psychology, as well as attitude and opinion change (Levine, 2000, 2003; Levine & Doyle, 2002), and goal-setting theory (Vancouver, et al., 2005). However, none of these applications are related to the psychological processes underlying individual risk perception and mitigating behavior.

The unit of analysis of the methodology is the feedback loop structure, i.e., the chains of reciprocal causal relations among the variables (Hirsch, et al., 2007). A SD model consists of a set of difference equations. Three types of variables are used. The first type of variable are 'stock variables' (conventionally represented in rectangles, as, for example, shown in Figure 4.6) Stocks represent accumulations over time. Psychological examples of stocks are constructs such as attitudes, self-esteem, expectations, anger, stereotypes, prejudices, trust, or beliefs (Carver & Scheier, 1982; Hirsch, et al., 2007; Levine, et al., 1992). Mathematically, the stocks represent integrations of their in- and outflows. 'Flows' are the second type of variable (depicted as horizontal arrows, cf. Figure 4.6). They feed into the stocks, as for example the change of attitudes. And third, auxiliary variables are used to mathematically conceptualize the in- and outflow rates. In analogy to traditional psychological analyses, stocks can be understood as the level of constructs or scales as, for instance, investigated by an ANOVA. The corresponding flows reflect change processes, e.g., the relations identified with regression analysis (Levine, et al., 1992). We followed the convention of standardizing the range of psychological stock variables on a scale from 0 to 100. In this way the values can be understood as percentages (Levine, 2000).

Due to the explicit distinction between stocks and flows, SD models can detail the development of stocks over time. At the same time, this temporal comprehension leads to difficulties in the implementation of psychological processes, since classical psychological theories do not provide insights into the time required to change stocks. More research is needed to determine these characteristics of psychological processes. The time units used for this model should not be regarded as an empirical specification of reality; rather, they indicate the number of iterations of the model required to arrive at the results.

With regard to the validation of our model, we have applied conventions in the field of SD (Levine, et al., 1992; Schwaninger & Groesser, 2008; Sterman, 2000) and report afterwards the sensitivity test of the model, and its ability to replicate the extracted theory-driven propositions regarding behavior change.

4. Specification and testing of the mathematical model of individual threat control

This section presents the specification and testing of the mathematical model explaining individual threat control. In a first step, the two competing dynamic core structures – the goal-

seeking versus the goal-avoiding feedback structure – are compared. This first comparison was made on a formal level without specifying the structural elements to the issue of threat control. Next, the proposed mathematical model of individual threat control is specified and tested on its validity. Finally, this model was used to explore the impact of external manipulations on individual IS security behavior.

4.1. Comparing the two alternative core model structures – the goal-seeking versus the goal-avoiding feedback loop

The main difference between the control-theoretical frameworks presented above is the nature of the proposed dynamic core structure. The TTAT posits a goal-avoiding feedback structure, whereas the PCT and the RHT describe a goal-seeking loop. These two alternative core model structures were translated into mathematical SD models and compared with regard to the behavioral simulations they produce.

Formulation of the goal-seeking and goal-avoiding feedback loop

The mathematical formulations of the two competing feedback structures closely followed the mathematical propositions of the PCT. Table 4-1 gives an overview of how the single elements of the PCT were formulated into the two SD model structures, and how the models were depicted with the Vensim software. The second column summarizes the outlines of the PCT from theoretical section 2.2. The third column presents the SD formulation of the goal-seeking feedback loop, and the fourth column that of the goal-avoiding feedback loop.

The SD formulation of the goal-seeking feedback loop differed from the PCT in only two aspects. First, the input quantity was divided into a stock q_i and a corresponding flow variable *change* q_i. Second, the impact of the external disturbance q_d was specified by applying the PULSE-function. This function operates by inducing the disturbance q_d at the start time (in the first position in the parentheses), over the time units specified at the second position in the parentheses.

Conversely to the goal-seeking feedback loop, the formulation of the goal-avoiding feedback loop assumed the error sensitivity factor S to correspond to the tolerance level proposed by the TTAT. Only if the error signal e falls below that value is the output quantity q_o activated. In this case, the impact of e on q_o has to be inversely proportional, as proposed by the TTAT:

$$q_{0_t} = IF\_THEN\_ELSE(e_t < S, \frac{1}{|e_t| + 1}, 0) \qquad \text{(Eq. 5)}$$

The IF THEN ELSE-function returns the first value (in the second position in the parentheses) if the condition (in the first position in the parentheses) is true, and the second value (in the third

position in the parentheses) if the condition is false. To ensure that the output quantity q_o remains above 0, even in the case of a perceptual signal p exceeding the reference value p^*, the error signal e was restricted to its absolute value. The addition of 1 in the numerator guaranteed that the latter remained unequal to zero.

Furthermore, the goal-seeking and the goal-avoiding feedback structure differed in the polarities of the impacts of the output quantities q_o and disturbing factors D. Within the goal-seeking structure, the output quantity is meant to approach the perceptual signal to the goal, and the external disturbance to enlarge this distance, whereas within the goal-avoiding structure, the output quantity should enlarge the distance, and an external disturbance re-approach the perceptual signal to the reference value.

Comparing the simulated model behavior of the goal-seeking and goal-avoiding feedback structure

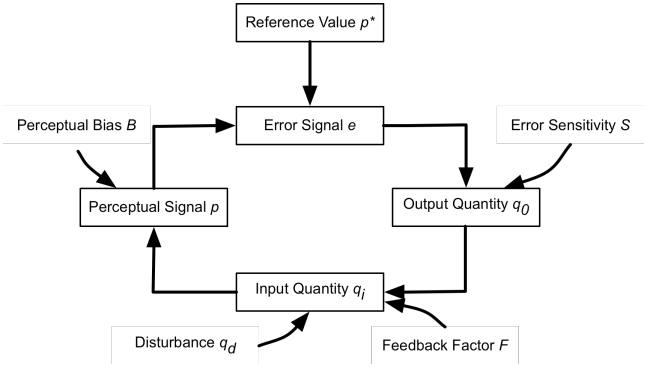
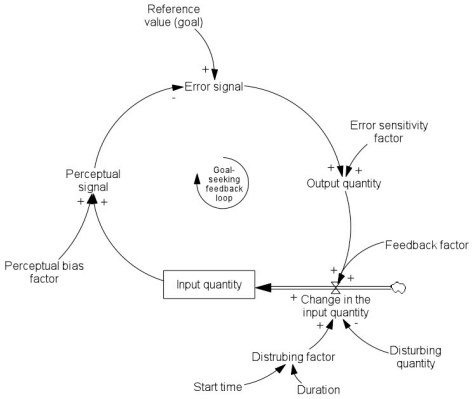
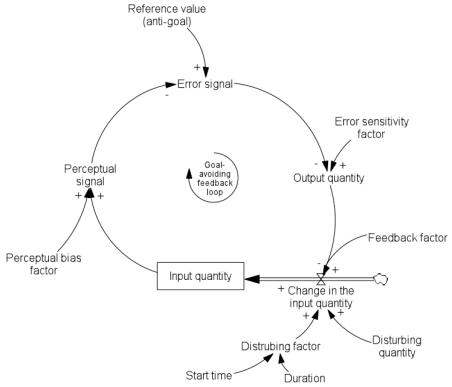
To test the behaviors of the models, different simulation runs were calculated over a period of 100 time units. For the different simulation runs, the initial values of the input quantity were varied, as well as whether or not an external disturbance q_d was introduced at t=60. Furthermore, for the goal-avoiding feedback model, the activation of a tolerance level (error sensitivity factor) was varied. The resulting progressions of the levels of the input quantity of the different simulation runs are shown in Figure 4.5.

Both models produced plausible behaviors. The goal-seeking structure reconciled the level of the input quantity with that of the reference value, for levels of the input quantity initially exceeding the reference value (runs 1-3 in Figure 4.5) as well as for those which initially went below the reference value (run 4). In the latter case, the progression of the input quantity changed direction, i.e., increased, similar to a risk-compensating behavior.

The goal-avoiding structure enlarged the distance of the input quantity from the reference value infinitely (runs 3 and 4), or until the distance equaled the introduced tolerance level (runs 1 and 2). However, this structure produced only one behavioral direction, namely a decrease in the input quantity. This phenomenon was intended for both situations, an initial level of the input quantity exceeding the reference value (run 1), as well as for input quantities lower than the reference value (runs 2-4). However, as a result, the structure did not compensate for the distance produced by an introduced external disturbance (run 2). Thus, with the goal-avoiding structure, the modeling of a risk-compensating behavior was not possible.

Furthermore, within the goal-avoiding structure, the reference value p^* no longer indicated the direction to the development of the input quantity q_i. This function was partly taken over by the error sensitivity factor S. As a consequence, the progressions of q_i of the goal-avoiding structure with introduced tolerance level showed a strong similarity to those produced by the goal-seeking structure (cf. run 2).

Table 4-1: Mathematical specification of the goal-seeking and a goal-avoiding feedback loop

Structural elements	***Specification of the PCT (cp. section 2.2)***	***SD specification of the goal-seeking loop***	***SD specification of the goal-avoiding loop***
			
Reference Value p^*	constant	15	20
Error Signal e	$p^* - p$	$p^* - p_t$	$p^* - p_t$
Error Sensitivity Factor S	constant	0.1	varied
Output Quantity q_o	$S * e$	$S * e_t$	$q_{0_t} = IF\_THEN\_ELSE(e_t < S, \frac{1}{\lvert e_t \rvert + 1}, 0)$
Feedback Factor F	constant	1	1
Disturbance q_d	constant	varied	varied
Disturbing Factor D	constant	*PULSE (start time, duration)*	q_d * *PULSE (start time, duration)*
Input Quantity q_i	$F * q_o - D * q_d$	$q_i = \int_{t_0}^{t} (change_{q_i}, q_{i_{t_0}})$	$q_i = \int_{t_0}^{t} (change_{q_i}, q_{i_{t_0}})$
Change in the input quantity $change_{qi}$	-	$F * q_{0_t} - D * q_d$	$D * q_d - F * q_{0_t}$
Perceptual Bias B	constant	1	1
Perceptual Signal p	$B * q_i$	$B * q_{i_t}$	$B * q_{i_t}$
Start time t	-	60	60
Duration	-	1	1

Note: For the behavior simulation, the constants in the PCT model (second column) were replaced by the values reported in the third column (for goal-seeking behavior) and fourth column (for goal-avoiding behavior).

These two weaknesses of the goal-avoiding feedback structure, and the fact that the formalization of the goal-seeking feedback structure is more explicit and parsimonious, disfavor the goal-avoiding structure. Therefore, as will be presented in the following section, we based our proposed model of individual threat control on the goal-seeking feedback structure.

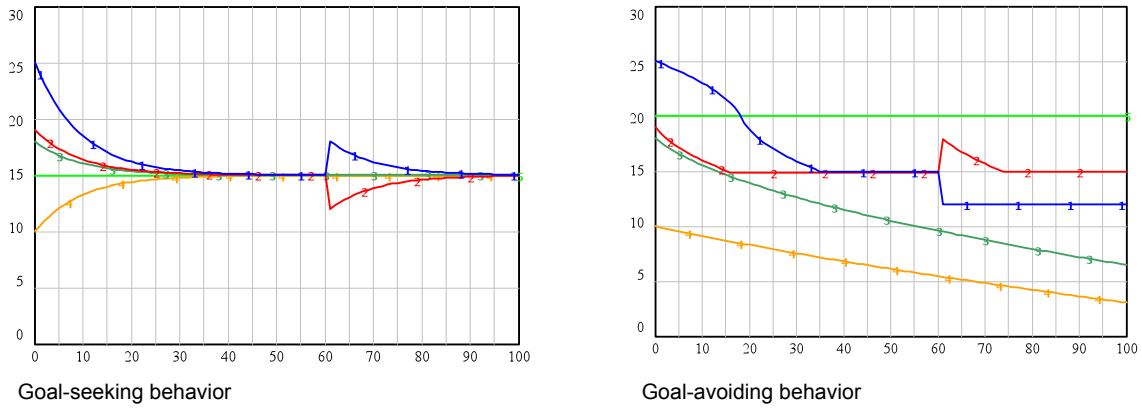


Figure 4.5. Progression of the level of the input quantity q_i in different simulation runs of the goal-seeking structure (on the left), and goal-avoiding structure (on the right).

Notes: X-axis = time units, Y-axis = level of q_i.

Line (1): Run 1: initial value of q_i = 25, q_d = -3, S = 5 for the goal-avoiding feedback loop, 0.1 for the goal-seeking feedback loop

Line (2): Run 2: initial value of q_i = 19, q_d = 3, S = 5 for the goal-avoiding feedback loop, 0.1 for the goal-seeking feedback loop

Line (3): Run 3: initial value of q_i = 18, q_d = 0, S = 100 for the goal-avoiding feedback loop, 0.1 for the goal-seeking feedback loop

Line (4): Run 4: initial value of q_i = 10, q_d = 0, S = 100 for the goal-avoiding feedback loop, 0.1 for the goal-seeking feedback loop

Line (5): Reference values: for all runs, 15 for the goal-seeking feedback loop, 20 for the goal-avoiding feedback loop

For all indications not reported in the figure caption, cf. Table 4-1.

4.2. Specification and validation of the mathematical model of individual threat control

The model of individual threat control we propose extends the goal-seeking feedback structure, described in the preceding section, with the theoretical elements described in section 2.4. In the following, its mathematical specification is described, before we turn to the presentation of the testing of the model sensitivity, and its validation against the theoretical behavior propositions from section 2.5.

Specification of the mathematical model of individual threat control

We translated the theoretically derived model from section 2.4 into a computational SD-model. Figure 4.6 depicts the counterpart of Figure 4.4, sketched with the Vensim software. The full documentation of the mathematical equations is provided in Appendix D.

The mathematical model consists of four stock variables (shown as rectangles in Figure 4.6), i.e., the 'Tolerated Threat Threshold', the 'Individual IS Security Behavior', the 'Perceived Overall Threat', and the 'Perceived Coping Efficacy'. These four elements are seen as representations of levels, which accumulate in- and outflows over time. The changes in these levels are regulated by four corresponding flow variables (shown as horizontal double-sided arrows in Figure 4.6), namely the 'net change in the tolerated threat threshold', the 'net change in the individual IS security behavior', the 'net change in the perceived overall threat', and the 'net change in the perceived coping efficacy'.

Threat control loop: We start with 'Perceived Overall Threat'. A change in this element may trigger the threat appraisal process. The level of 'Perceived Overall Threat' is compared with previously undertaken security measures, i.e., with 'Individual IS Security Behavior', in order to estimate the 'perceived non-covered threat'. This comparison is delayed by the time needed to adjust the perception: the 'time to perceive the non-covered threat'.

The 'perceived non-covered threat' is compared with the 'Tolerated Threat Threshold' in order to estimate the 'discrepancy'.

The threat-control loop continues with the link from the 'discrepancy' to the 'protective motivation'. How precisely, 'protective motivation' is affected by the two appraisal processes, relating to threat and coping efficacy, has been discussed extensively (Cismaru & Lavack, 2007; Eagly & Chaiken, 1993; Rogers & Prentice-Dunn, 1997; Witte & Allen, 2000). The empirically found interactions between the perceived threat and coping efficacy favor a multiplicative relationship. We understand 'Perceived Coping Efficacy' to correspond to an expectancy assessment about how quickly the 'discrepancy' can be reduced. Therefore, the absolute level of 'Perceived Coping Efficacy' has to be translated into a weight ranging from 0 to 1. Further, the level of 'Perceived

Coping Efficacy' is only relevant if there is an intended increase in 'Individual IS Security Behavior', i.e., in the case of a positive 'discrepancy', but is unrelated to a decrease in 'Individual IS Security Behavior' in the case of a negative 'discrepancy'. These considerations are formalized as follows:

$$\begin{aligned} &\textit{protective motivation}_t = \textit{discrepancy}_t \\ &* \textit{IF THEN ELSE (discrepancy}_t < 0, 1, \textit{Perceived Coping Efficacy}_t * 0.01) \end{aligned} \quad \text{(Eq. 6)}$$

Given the time delay needed to implement the intended behavior change ('time to change the individual IS security behavior') the 'protective motivation' affects the 'net change in the individual IS security behavior'. With this, the threat-control loop is closed.

Goal-adjustment loop: Within the goal-adjustment loop, 'defensive motivation' is assumed to be the product of 'discrepancy' and the inverse effect of 'Perceived Coping Efficacy':

$$\begin{aligned} &\textit{defensive motivation}_t = \textit{discrepancy}_t \\ &* \textit{IF THEN ELSE (discrepancy}_t < 0, 1, \textit{(100-Perceived Coping Efficacy}_t)*0.01) \end{aligned} \quad \text{(Eq. 7)}$$

'Defensive motivation', in turn, impacts on the 'net change in the tolerated threat threshold'. With this, the goal-adjustment loop is also closed.

External impacts: The core model, as described so far, has been extended by three external impact options on the net changes in the three stock variables 'Tolerated Threat Threshold', 'Perceived Overall Threat', and 'Perceived Coping Efficacy'. These three impact options allow change policies to be simulated. Each external impact contains three components: the strength of the corresponding external impact, the time at which the impact is meant to begin (start time), and the duration of the external impact (time duration). To facilitate understanding, the effects of the three external impacts on the corresponding stock variables are depicted in Figure 4.7. For all three examples external impacts were introduced with the same strength (magnitude of 10), at the same time (start time = 10), and over the same duration (2 time units).
'External impact on the tolerated threat threshold' is assumed to change the 'Tolerated Threat Threshold' permanently, as shown in Figure 4.7a. In contrast, the external impact on 'Perceived Overall Threat' is assumed to evoke only a short-lasting change, maintained for approximately as long as the altered (or reduced) external impact holds, as shown in Figure 4.7b. This is modeled by an additional goal-seeking feedback loop, whose reference value consists of the size of the altered external overall threat towards which 'Perceived Overall Threat' approached.

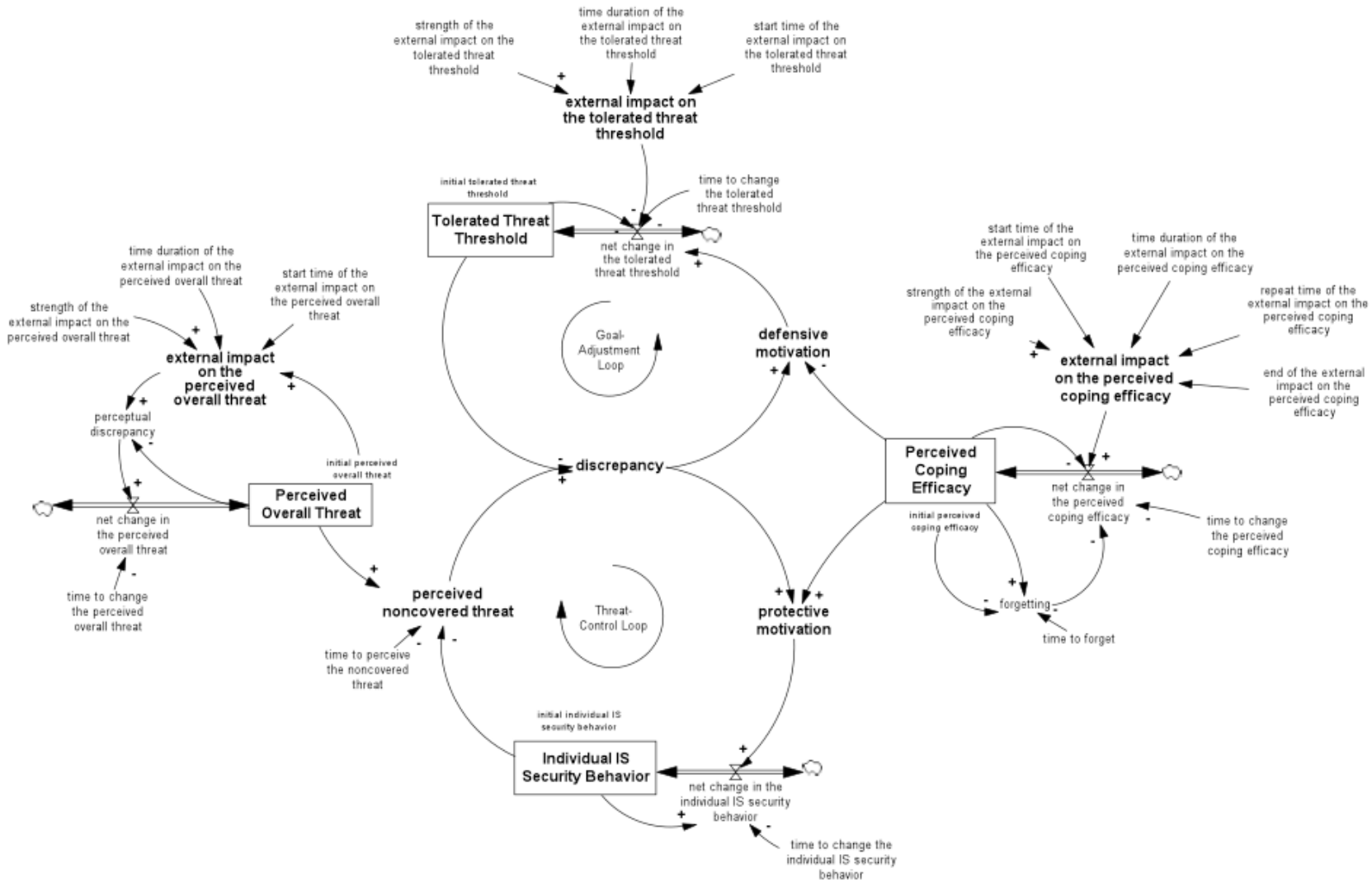


Figure 4.6. SD representation of the model of individual threat control as sketched using the Vensim software

The 'external impact on the perceived coping efficacy' is understood to be maintained longer than that on 'Perceived Overall Threat'. However, in contrast to the impact on 'Tolerated Threat Threshold', it was assumed that the effect of an external policy on 'Perceived Coping Efficacy', such as improved skills acquired in a training program, is not permanent. Therefore, the auxiliary 'forgetting' has been introduced, to decrease the enhanced 'Perceived Coping Efficacy' to its initial level. Other than the two external impacts described above, the impact on 'net change in the perceived coping efficacy' is supplemented with the option of a repetition. This repetition starts after a time period defined by 'repeat time of the external impact on the perceived coping efficacy', and ends at 'end of the external impact on the perceived coping efficacy'. In Figure 4.7c, 'external impact on the perceived coping efficacy' was repeated once after 10 time units.

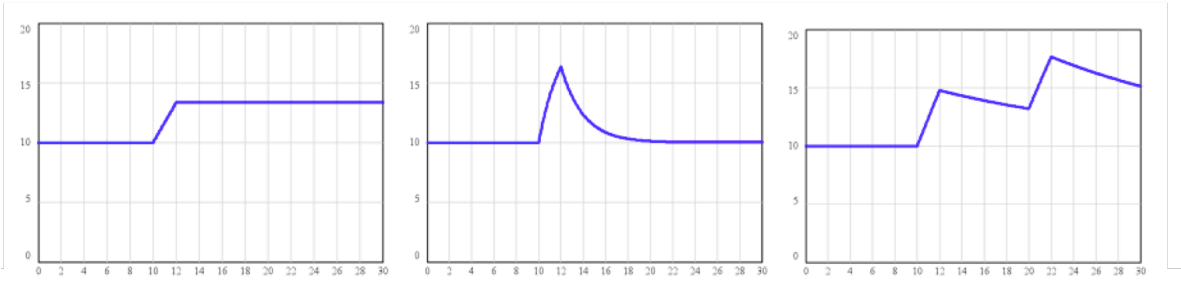


Figure 4.7. Simulations of the external impacts, changing the levels of the three stock variables 'Tolerated Threat Threshold' (a), 'Perceived Overall Threat' (b), and 'Perceived Coping Efficacy' (c).

Notes. X-axis = time units, y-axis = levels of the stock variables. For all three simulations, the initial values of the three stock variables were set to 10, the strengths of the impacts to 10, the start times to 10, and the durations of the impacts to 2. For 'Perceived Coping Efficacy' (c) the impact was repeated once after 10 time units. Delays were set to 6 for 'time to change the tolerated threat threshold', 2 for 'time to change the overall threat', 4 for 'time to change the perceived coping efficacy', and 20 for 'time to forget'.

Time delays: The modeling approach SD accounts for changes in the entities considered over time. This is reasonable since the perception of an environmental situation, the implementation of a behavior change, and the gradual adjustment of values or principles occurs over time. We thus explicitly consider time delays in the model. The assumption of a goal hierarchy implies that higher-order levels respond more slowly and are more resistant to change than lower-level concepts (Carver, 2006; Powers, 1973). Thus, we assume:

time to change the tolerated threat threshold > time to change the individual IS security behavior (Eq. 8)

For concepts on the same hierarchical level, the evaluation of relative time delays is less clear. We suppose implementing a behavior change takes more time than perceiving a changing threat.

In other words, behavior changes require time for preparation and the right moment to be implemented whereas reappraising the threat in light of the assumed behavioral effect is a cognitive activity, which can occur within a moment. Thus, we propose that it takes less time to perceive a non-covered threat than to change security behavior:

time to change individual IS security behavior > time to perceive the non-covered threat (Eq. 9)

Correspondingly, the ranking of the external impact time delays were assumed as follows:

time to change the perceived overall threat < time to change the perceived coping efficacy (Eq. 10)
time to change the perceived coping efficacy < time to change the tolerated threat threshold (Eq. 11)
time to the change tolerated threat threshold < time to forget (Eq. 12)

Test of the model sensitivity

Sensitivity analysis was used to test the robustness of the model behavior when initial values are varied over a plausible range of parameter values. Therefore, the initial values of the four stock variables 'Tolerated Threat Threshold', 'Perceived Coping Efficacy', 'Individual IS Security Behavior', and 'Perceived Overall Threat' were ranged from 0 to 100, and 200 simulation runs were randomly calculated in a Monte Carlo Simulation of Sensitivity. Potential external impacts were omitted for the sensitivity analysis. The delays were set to '1' for 'time to perceive the non-covered threat', '4' for 'time to change the individual IS security behavior', and '6' for 'time to change the tolerated threat threshold'. With this calibration of the time delays 'Individual IS Security Behavior' reached the level of 100 under ideal conditions, i.e., initial values of 'Perceived Overall Threat' and 'Perceived Coping Efficacy' of '100', and of 'Tolerated Threat Threshold' of '0' (cf. the blue line in Figure 4.8a). This default for the time delays was consequently used for all simulation runs reported in this chapter.

The behaviors of the stock variables 'Individual IS Security Behavior' and 'Tolerated Threat Threshold', shown in Figures 4.8a and b, were particularly interesting, because they were affected by the changing initial values. In all tested runs the levels of the two stock variables remained as intended within the range between 0 and 100.

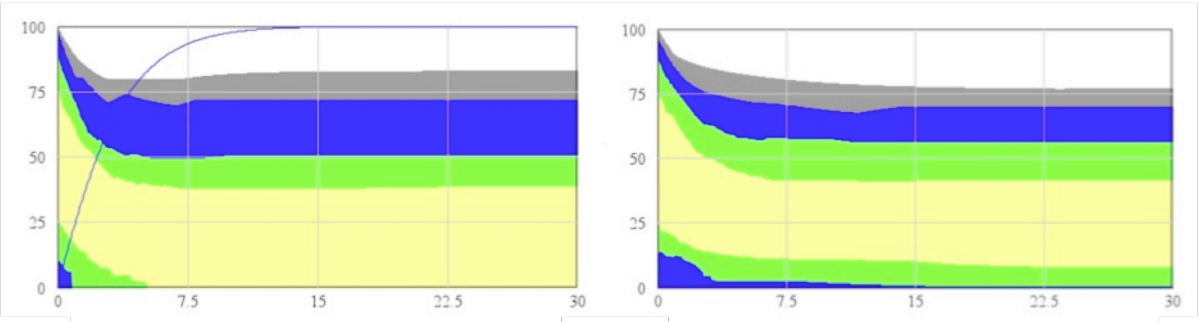


Figure 4.8. Progression of the levels of the stock variables 'Individual IS Security Behavior' (a) and 'Tolerated Threat Threshold' (b) in the sensitivity test.

Notes: 200 simulation runs were calculated in a Monte Carlo simulation of sensitivity when varying the initial values of all stock variables from 0 to 100, drawn from random uniform distributions. The Y-axis shows the level of the corresponding stock variables; the X-axis represents the time units. Colors correspond to the confidence intervals of the resulting levels of the stock variables, with ■ 50%, ■75%, ■ 95%, and ■ 100%. The thin blue line (in graph a) corresponds to the development under ideal conditions (initial values of 'Tolerated Threat Threshold' and 'Individual IS Security Behavior' = 0, initial values of 'Perceived Overall Threat' and 'Perceived Coping Efficacy' = 100, 'time to perceive the non-covered threat = 1, 'time to change individual IS security behavior' = 4, 'time to change the tolerated threat threshold' = 6).

Validating the model behavior using the theoretical propositions on behavior change

Next, we tested whether our model of individual threat control could reproduce behavior changes as they are described by the theoretical propositions on behavior change. Table 4-2 resumes the theoretical propositions from section 2.5 and summarizes the corresponding findings. The comparison was made by running the model over a phase of 30 time units under different combinations of the initial values of the stock variables: The initial value of 'Perceived Coping Efficacy' was varied from high (90) to low (10), that of 'Tolerated Threat Threshold' from low (10) to moderate (50), and that of 'Perceived Overall Threat' from high (90) to moderate (40). We favored moderate initial values of 'Tolerated Threat Threshold' and 'Perceived Overall Threat' over extreme values, as moderate levels were assumed to better match real situations. For all simulation runs, the initial value of 'Individual IS Security Behavior' was set to 10. Potential external impacts were omitted for the reproduction of the propositions.

The outcomes of the different simulation runs are shown in Figure 4.9. Compared to a moderate initial value of 'Tolerated Threat Threshold', a low initial value of this stock produced a higher level of 'Individual IS Security Behavior' at t=30. This finding replicated the first proposition (P1) and held true under high and moderate 'Perceived Overall Threat' (run 1 vs. 5, and 3 vs. 7 in Figure 4.9), as well as under high and low 'Perceived Coping Efficacy' (run 2 vs. 6, and 4 vs. 8 in Figure 4.9).

Table 4-2: Comparison of the theoretical propositions and the results of the model simulation

Theoretical Proposition on Behavior Change from section 2.5		***Results of the model simulation***
P1	A low threshold of tolerated threat results in a higher individual IS security behavior than a high threshold of tolerated threat.	Replicated (cf. comparisons of the runs 1 vs. 5, 2 vs. 6, 3 vs. 7, and 4 vs. 8 in Figure 4.9)
P2	A high level of perceived overall threat provokes a higher level of individual IS security behavior than a low level of perceived overall threat	Replicated (cf. comparisons of the runs 1 vs. 3, 2 vs. 4, 5 vs. 7, and 6 vs. 8 in Figure 4.9)
P3	A high level of perceived coping efficacy results in higher level of individual IS security behavior than a low level of perceived coping efficacy.	Replicated by the comparisons of the runs 1 vs. 2, 3 vs. 4, 5, vs.6, not replicated by the comparison of the runs 7 vs. 8 in Figure 4.9)
P4	The resulting level of individual IS security behavior should be highest under the condition in which a high level of perceived overall threat is combined with a high level of perceived coping efficacy and lowest under the condition in which a low level of perceived overall threat is combined with a low level of perceived coping efficacy.	Replicated (cf. Figure 4.10)
P5a	The perception of an overall threat level exceeding the tolerated threat threshold provokes an increase in the level of the individual IS security behavior, i.e., a threat-controlling behavior.	Replicated (cf. Runs 1-6 in Figure 4.9)
P5b	The perception of an overall threat level lower than the tolerated threat threshold provokes a decrease of the level of individual IS security, i.e., a threat-compensating behavior.	Replicated (cf. Runs 7-8 in Figure 4.9)
P6	The resulting threshold of tolerated threat should be highest under the condition in which a high level of perceived overall threat is combined with a low level of perceived coping efficacy, and lowest under the condition in which a low level of perceived overall threat is combined with a high level of perceived coping efficacy.	Replicated (cf. Figure 4.11)

The second proposition (P2) was also confirmed: a high initial 'Perceived Overall Threat' resulted in a higher 'Individual IS Security Behavior' (runs 1, 2, 5, 6 in Figure 4.9) than a moderate initial level (runs 3, 4, 7, 8) in all bivariate comparisons.

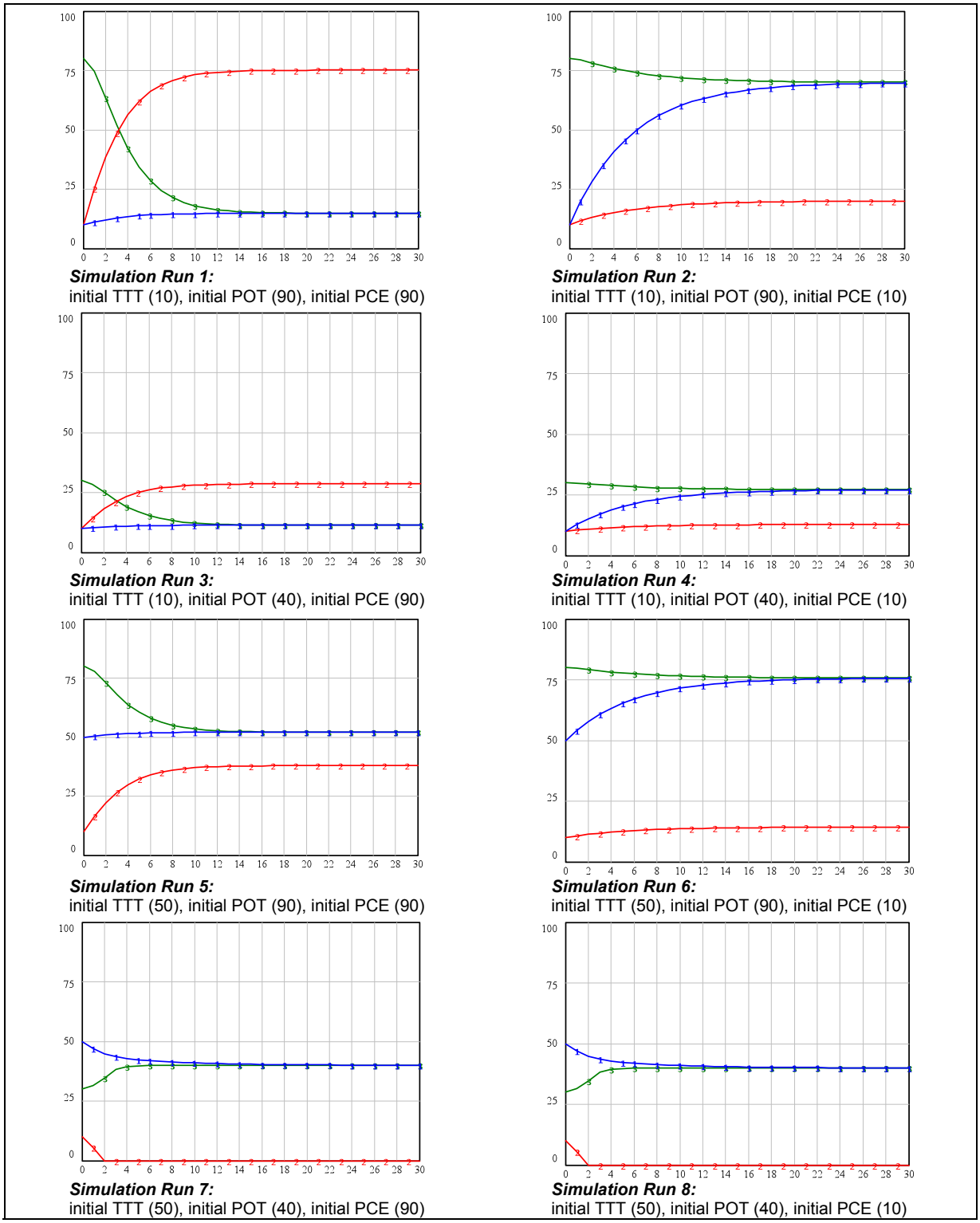


Figure 4.9. Model simulation of varying initial values of 'Tolerated Threat Threshold' (TTT), 'Perceived Overall Threat' (POT), and 'Perceived Coping Efficacy' (PCE).

Notes: Y-axis shows the level of the corresponding stock variables, X-axis represents the time units. For all simulation runs, the initial level of 'Individual IS Security Behavior' was set to 10. POT and PCE were omitted in the graphical depiction of the simulation runs, as they remained constant over the time.

Line (1): Level of 'Tolerated Threat Threshold'

Line (2): Level of 'Individual IS Security Behavior'

Line (3): Level of the 'perceived non-covered threat'

Moreover, the third proposition (P3) was also generally replicated: In three of the four comparisons, a high initial value of 'Perceived Coping Efficacy' resulted in a higher 'Individual IS Security Behavior' (runs 1, 3, 5 in Figure 4.9) than the low initial value (runs 2, 4, 6). Exceptions were the two runs in which the initial level of 'Perceived Overall Threat' was lower than that of 'Tolerated Threat Threshold' (runs 7 and 8). In these two runs the model reduced the 'discrepancy' similarly quickly by lowering the security level until it reached the minimum value. Thus, the model also reproduced propositions 5a and 5b: A 'Perceived Overall Threat' exceeding the 'Tolerated Threat Threshold' provoked an increase in 'Individual IS Security Behavior' (runs 1-6), whereas a 'Perceived Overall Threat' below the 'Tolerated Threat Threshold' resulted in risk-compensating behavior (runs 7 and 8).

To test the proposed interaction effect of 'Perceived Overall Threat' and 'Perceived Coping Efficacy' (P4), additional simulations were calculated by varying the initial value of 'Perceived Overall Threat' (0-100), and 'Perceived Coping Efficacy' (10 vs. 90). The initial values of 'Tolerated Threat Threshold' and 'Individual IS Security Behavior' were set to 10. Figure 4.10 depicts the final values of 'Individual IS Security Behavior' at t=30 in these simulation runs.

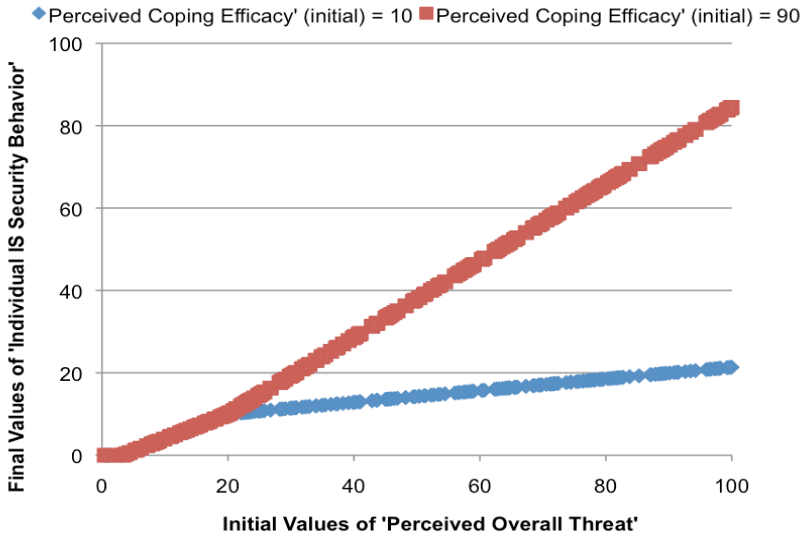


Figure 4.10. Final values of 'Individual IS Security Behavior' of 500 simulation runs, in which the initial values of 'Perceived Overall Threat' (0-100) and 'Perceived Coping Efficacy' (10 vs. 90) were varied.

Note: The initial values of 'Tolerated Threat Threshold' and 'Individual IS Security Behavior' were set to 10.

A 'discrepancy' of zero was obtained with a 'Perceived Overall Threat' of 20, taking into account the initial values of 'Tolerated Threat Threshold' (10) and 'Individual IS Security Behavior' (10). As soon as a positive 'discrepancy' emerged (greater than 20 for 'Perceived Overall Threats'), the assumed interaction could be replicated: the resulting 'Individual IS Security Behavior' was low-

est under the low threat – low coping efficacy condition and highest under the high threat – high coping efficacy condition.

When 'Perceived Overall Threat' was lower than 20, 'perceived non-covered threat' fell below the 'Tolerated Threat Threshold' and thus produced a negative 'discrepancy'. In this case, the discrepancy was compensated for by lowering 'Individual IS Security Behavior'.

Figure 4.11 depicts the final values of 'Tolerated Threat Threshold' at t=30 under the same variation of the initial values of 'Perceived Overall Threat' and 'Perceived Coping Efficacy' as mentioned above. The adjustment of 'Tolerated Threat Threshold' yielded a trend analogous to that of 'Individual IS Security Behavior'. The strongest emotion-focused reaction, i.e., the highest final 'Tolerated Threat Threshold', emerged when the initial value of 'Perceived Overall Threat' was high and the initial value of 'Perceived Coping Efficacy' was low. The model showed the weakest reaction in the case of a low initial value of 'Perceived Overall Threat' and high initial value of 'Perceived Coping Efficacy'. Thus, the model behavior replicated the theoretically proposed interaction (P6).

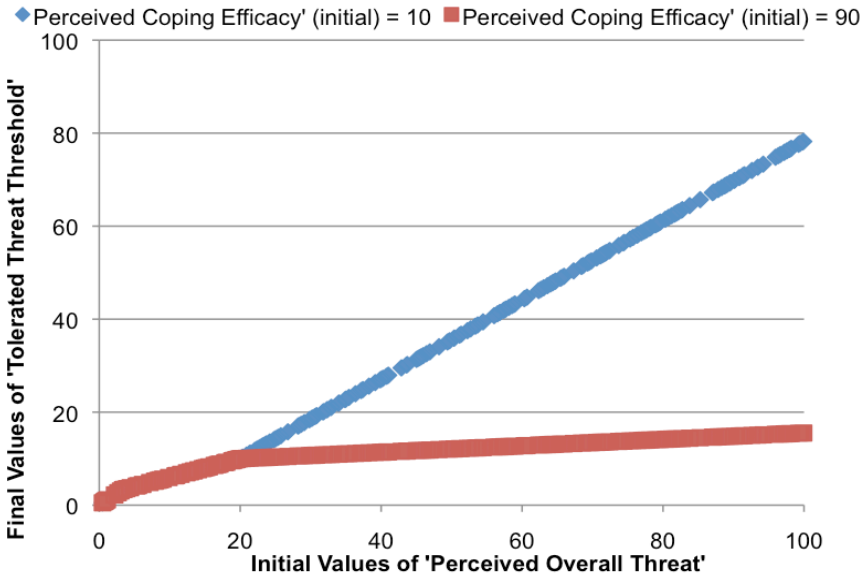


Figure 4.11. Final values of 'Tolerated Threat Threshold' of 500 simulation runs, in which the initial values of 'Perceived Overall Threat' (0-100) and 'Perceived Coping Efficacy' (10 vs. 90) were varied.

Note: The initial values of 'Tolerated Threat Threshold' and 'Individual IS Security Behavior' were set to 10.

4.3. Exploring targeted manipulation of the external impacts to increase the level of individual IS security behavior

As a final step, the computational model was used to explore the effects of changes in the external impacts on individual IS security behavior. The aim was to find out which combinations of

external impacts resulted best in an increase of the security behavior level. The manipulation of the external impacts was combined with different initial conditions as used in the simulations described in the preceding section (cf. Figure 4.9). We considered only conditions with an initially moderate level of 'Perceived Overall Threat'. This selection results from the assumption that a constantly high current level of external danger is not found in reality. More realistically, such situations emerge from a temporary amplification of available risk information. Thus, from the simulation runs in Figure 4.9, the third, fourth, and seventh were chosen for further analysis. These three simulation runs represent three ideal-typical reaction possibilities of individuals in threatening situations:

Type I: The first type corresponds to simulation run 3 in Figure 4.9. This type enjoys almost ideal premises to cope with threats, i.e., he or she has a low 'Tolerated Threat Threshold' and a high 'Perceived Coping Efficacy'. For reasons of simplicity, we call this type the 'Risk Manager' in what follows.

Type II: The second type conforms to simulation run 4 in Figure 4.9. Conversely to the 'Risk Manager', this type perceives few options for coping with threats, i.e., he or she has a low 'Perceived Coping Efficacy'. Thus, this type is rather defenseless when exposed to threats - a 'Victim'.

Type III: And third, we focused on simulation run 7 in Figure 4.9. This type would have the required skills to cope with potential threats as he or she has high 'Perceived Coping Efficacy'. However, this type accords less value to IS security principles than to principles competing with the former, as assumed based on his or her moderate 'Tolerated Threat Threshold'. We suppose further that this type tends to use IT intensively, but mainly omits security measures, as he or she does not perceive any necessity for using them. Thus, this type constitutes a weakness of the IS security system, since he or she is a potential 'Risk Causer'.

Simulation run 8 of Figure 4.9 was not pursued, because a type which values high principles competing with security issues, and which simultaneously has low computer skills, is less intuitive.

In the following, these three simulation runs were repeated. External impacts were introduced in order to explore how an increase in 'Individual IS Security Behavior' may be achieved.

Effective manipulations of external impacts for the 'Risk Manager' (Type I)

The 'Risk Manager' is skilled in coping options and disposes over a low 'Tolerated Threat Threshold'. As shown in Figure 4.12, for this type, a temporary increase in the 'Perceived Overall Threat' is sufficient to enhance its security behavior. The initial phase (time 0-20) of the simulation run shown in Figure 4.12 corresponds to simulation run 3 in Figure 4.9. At t = 20, we introduced an 'external impact on the perceived overall threat' of strength 20 for ten time periods. The 'Risk Manager' reacted appropriately to the perceived increase of the overall threat by temporarily increasing its security behavior. After that, the 'Perceived Overall Threat' returned to its initial value; the security behavior level declined, however, returning to a level slightly higher than the one previous to the manipulation, due to a small decrease in the 'Tolerated Threat Threshold'.

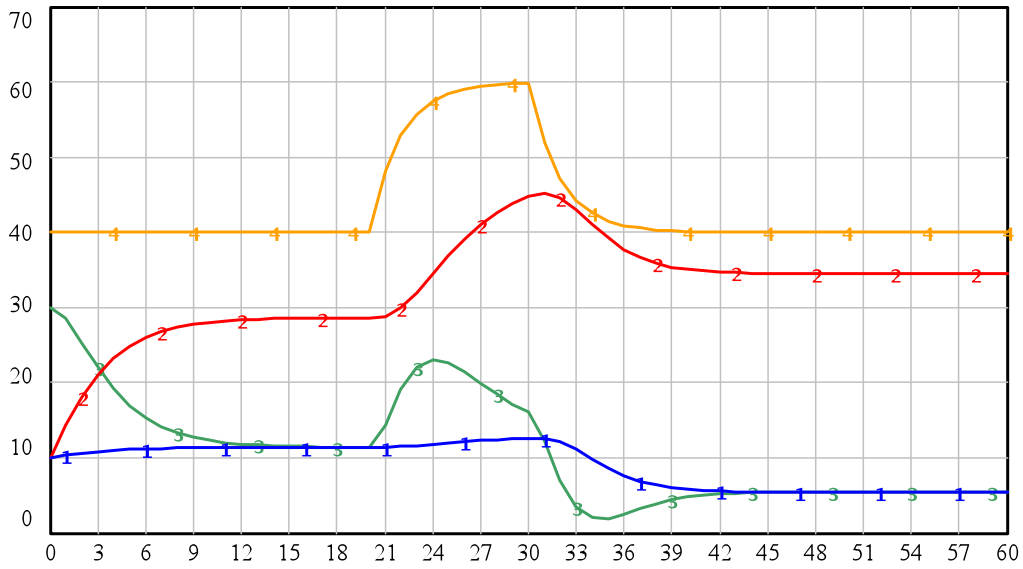


Figure 4.12. Simulation of the behavior reaction of the 'Risk Manager' to an externally induced increase of 'Perceived Overall Threat'.

Notes: The Y-axis shows the level of the corresponding variables; the X-axis represents the time units. Time units 1-20 correspond to those in simulation run 3 in Figure 4.9. The external manipulation was defined as follows: 'Strength of external impact on perceived overall threat' = 20, 'start time' = 20, 'time duration' = 10

Line (1): Level of 'Tolerated Threat Threshold'

Line (2): Level of 'Individual IS Security Behavior'

Line (3): Level of 'perceived non-covered threat'

Line (4): Level of 'Perceived Overall Threat'

Effective manipulations of external impacts for the 'Victim' (Type II)

The type we named 'Victim' had a low 'Tolerated Threat Threshold', as well as a low 'Perceived Coping Efficacy'. Introducing the same manipulation as to the 'Risk Manager' above produced a

completely unintended reaction, as shown in the first picture in the left part of Figure 4.13: The main effect of an increased 'Perceived Overall Threat' was a rise in the 'Tolerated Threat Threshold', since this type reduced the discrepancy by adapting the goal.

The main deficit of this type lies in its low 'Perceived Coping Efficacy'. We therefore introduced in a next step an external impact on the 'Perceived Coping Efficacy' at t=50. However, this second attempt, shown in the middle section of Figure 4.13, also failed to increase 'Individual IS Security Behavior', as the equilibrium between the 'perceived non-covered threat' and the 'Tolerated Threat Threshold' had already been reached. Third, we introduced a reduction in the 'Tolerated Threat Threshold' at t = 110. As depicted in the last part of Figure 4.13, this manipulation slightly improved 'Individual IS Security Behavior'.

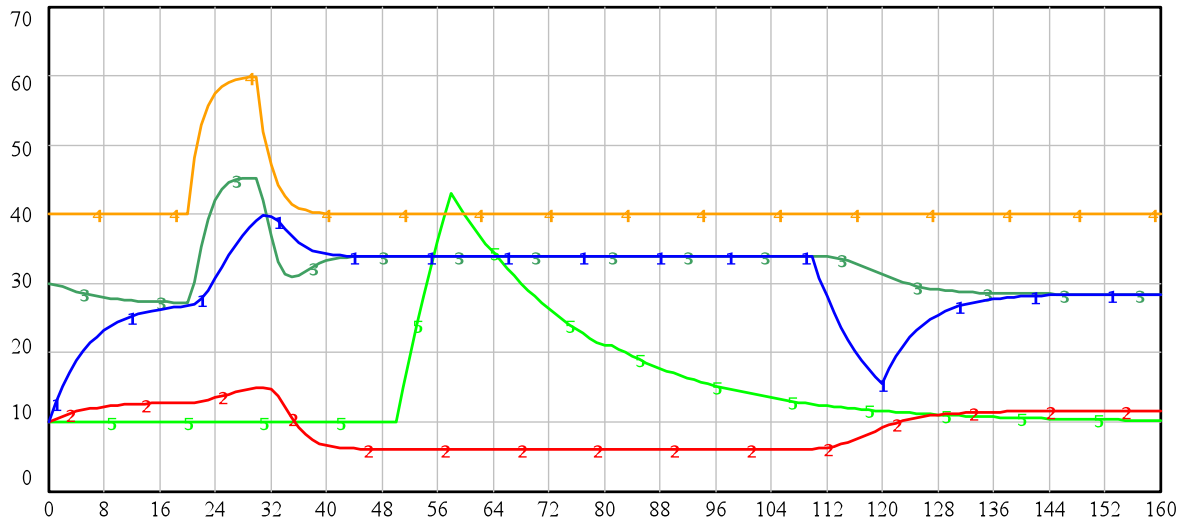


Figure 4.13. Simulation of behavior reactions of the 'Victim' to singular externally induced impacts on 'Perceived Overall Threat', 'Perceived Coping Efficacy', and 'Tolerated Threat Threshold'.

Notes: The Y-axis shows the level of the corresponding variables; the X-axis represents the time units. Time units 1-20 correspond to those in simulation run 4 in Figure 4.9. The external manipulations were defined as follows: strengths of the external impacts = 20, time durations = 10, start time of the external impact on perceived overall threat = 20, start time of the external impact on perceived coping efficacy = 50, and start time of the external impact on tolerated threat threshold = 110.

Line (1): Level of 'Tolerated Threat Threshold'

Line (2): Level of 'Individual IS Security Behavior'

Line (3): Level of 'perceived non-covered threat'

Line (4): Level of 'Perceived Overall Threat'

Line (5): Level of 'Perceived Coping Efficacy'

We therefore tried a combination of measures. As depicted in Figure 4.14, the 'Individual IS Security Behavior' of the 'Victim' was best supported by first strengthening, the security principles

(decreasing the 'Tolerated Threat Threshold' at t=40) combined with a simultaneous training of the coping skills (increase of the 'Perceived Coping Efficacy' at t=40). Only then was a subsequently introduced increase in the 'Perceived Overall Threat' (at t=80), optimally combined with a repeated increase in 'Perceived Coping Efficacy' (at t=80), converted into an enhanced persisting 'Individual IS Security Behavior'.

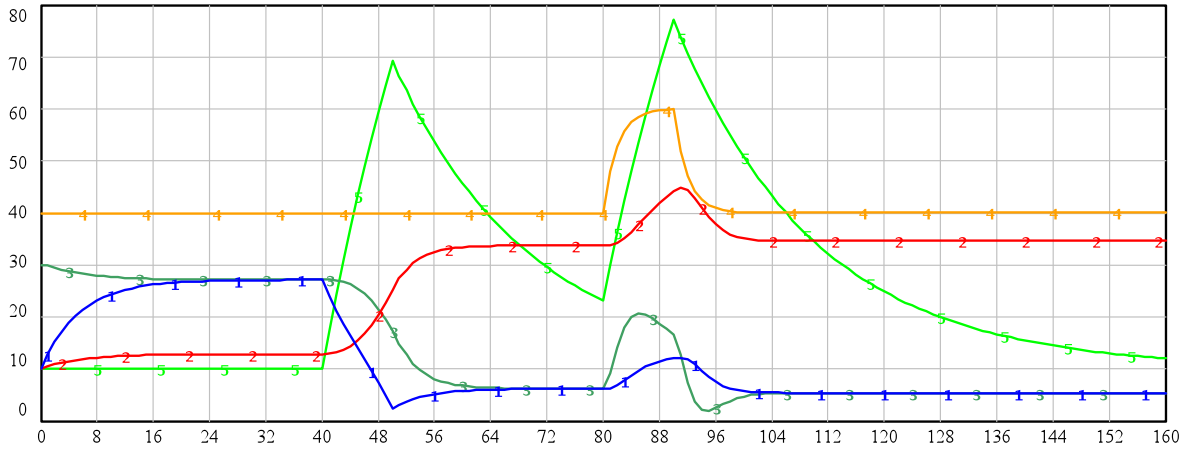


Figure 4.14. Simulation of behavior reactions of the 'Victim' to combined externally induced impacts on 'Perceived Overall Threat', 'Perceived Coping Efficacy', and 'Tolerated Threat Threshold'.

Notes: The Y-axis shows the level of the corresponding variables; the X-axis represents the time units. Time units 1-20 correspond to those in simulation run 4 in Figure 4.9. The external manipulations were defined as follows: strengths of the external impacts on perceived overall threat and on tolerated threat threshold = 20, strength of the external impact on perceived coping efficacy = 30, time durations = 10, start time of the external impact on tolerated threat threshold = 40, start time of the external impact on perceived coping efficacy = 40, repeat time = 40, end = 100, start time of the external impact on perceived overall threat = 80.

Line (1): Level of 'Tolerated Threat Threshold'

Line (2): Level of 'Individual IS Security Behavior'

Line (3): Level of 'perceived non-covered threat'

Line (4): Level of 'Perceived Overall Threat'

Line (5): Level of 'Perceived Coping Efficacy'

Effective manipulations of external impacts for the 'Risk Causer' (Type III)

The third type, the 'Risk Causer', perceives no necessity for security measures due to a relatively high 'Tolerated Threat Threshold'. Again, we explored how this type might react to a singular externally introduced increase in the 'Perceived Overall Threat' at t=20. The behavioral reaction is depicted on the left-hand side of Figure 4.15. Similar to the 'Risk Manager', the 'Risk Causer' reacted with an increase in 'Individual IS Security Behavior', albeit on a lower level.

The simulation of the exogenous increase in the 'Perceived Overall Threat' was repeated in a next step in combination with an exogenous decrease in 'Tolerated Threat Threshold'. As shown on the right-hand side of Figure 4.15, this intervention was more effective.

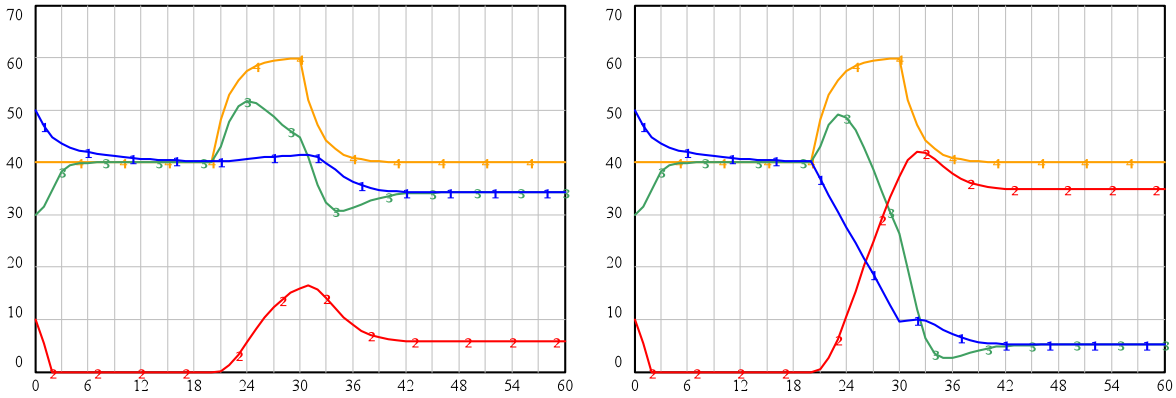


Figure 4.15. Simulation of behavior reactions of the 'Risk Causer' to singular (on the left), and combined (on the right) externally induced impacts on 'Perceived Overall Threat', and 'Tolerated Threat Threshold'.

Notes: The Y-axis shows the level of the corresponding variables; the X-axis represents the time units. Time units 1-20 correspond to those in simulation run 7 in Figure 4.9. The external manipulations were defined as follows: strengths of the external impacts = 20, time durations = 10, start time of the external impact on perceived overall threat = 20, start time of the external impact on tolerated threat threshold (only in the right picture) = 20

Line (1): Level of 'Tolerated Threat Threshold'

Line (2): Level of 'Individual IS Security Behavior'

Line (3): Level of 'perceived non-covered threat'

Line (4): Level of 'Perceived Overall Threat'

5. Discussion

The construction and test of dynamic models presents a promising extension to conventional unidirectional research on individual management of IS security risks. Such a dynamic process-oriented framework has been provided by the technology threat avoidance theory TTAT (Liang & Xue, 2009). The purpose of the present chapter was to elaborate the general propositions of the TTAT. This was done by integrating aspects of alternative control-theoretical frameworks, namely the perceptual control theory PCT (Powers, 1973, 1990), and the risk homeostasis theory RHT (Wilde, 1982b, 1998), as well as considerations on goal adjustment (Carey, 2008; Carver & Scheier, 1990; Rassmussen, et al., 2006; Scheier & Carver, 2003) into a new model of individual threat control. Its elements were theoretically specified, and the model was formulated as a mathematical working model.

In the next section, the model behavior is reconsidered, before we turn to the discussion of the limitations and open issues of our undertaking. We conclude with implications for further research and practice.

5.1. Summary and interpretation of the simulated model behavior

In a first step, a decision had to be made regarding the adequacy of the two competing dynamic core structures proposed by the different theoretical frameworks. The TTAT proposes a goal-avoiding feedback structure, whereas the RHT posits a goal-seeking feedback structure. The proposition of the TTAT was challenged from a theoretical as well as from a formal point of view. In particular, we questioned the theoretical suitability of the goal-avoiding structure to model cognitive appraisal processes, such as the appraisal of risk and coping efficacy (Rogers & Prentice-Dunn, 1997), as goal-avoiding behavior had been described as a first instinctive reaction to stimuli, and as a personality disposition (Carver & White, 1994; Elliot & Covington, 2001; Sherman, Mann, & Updegraff, 2006). We translated both proposed structures into mathematical working models. Comparison of the behavior simulations that were produced supported our preference for the goal-seeking feedback structure. The mathematical formulation of this structure was more elegant and parsimonious. Furthermore, this working model showed more options to model impacts per reference value and alternative behaviors, such as risk-compensating behavior (Wilde, 1982b, 1998).

In a second step, we proposed a new model of individual threat control, based on a goal-seeking structure. Its elements were theoretically specified, and again the model was translated into a mathematical working model. The simulated behavior yielded by the model was compared with propositions derived from theory. These theoretical propositions on individual IS security behavior changes were nicely replicated by simulated model behavior. Furthermore, we used the model for experimentation. This testing revealed interesting insights about essential preconditions for an increase in individual IS security behavior, which have largely been neglected by unidirectional frameworks. For example, as Wilde (1982b, 1998) theoretically assumed, the reference value in the form of a tolerated threat threshold determined the level of the resulting individual IS security behavior in all simulated conditions. It even emerged that a low tolerated threat threshold may be a necessity for other interventions to be effective, such as the increase in the perceived threat or coping efficacy. Based on theoretical frameworks on goal hierarchy (Carver & Scheier, 1982, 1990; Powers, 1973), we assumed the tolerated threat threshold to be a result of the awareness of IS security values and principles. The impact of such principles on individual IS security behavior has been repeatedly emphasized theoretically (Drevin, et al., 2007; Stewart, 2004), and recommendations have been elaborated regarding how to enhance security principles (Smith, 1989; Tsohou, Kikilakis, Karyda, & Kiountouzis, 2008). However, em-

pirical research has largely neglected the relationship between IS security principles and individual IS security behavior.

Surveys found that perceived IS security threats are positively correlated with protective motivations (Ng, et al., 2009; Workman, 2007; Workman, et al., 2008). This phenomenon was replicated by the simulated model behavior: a high level of perceived overall threat produced a higher level of individual IS security behavior rather than a low level of perceived overall threat. Furthermore, this difference in the resulting individual IS security behavior was higher under high perceived coping efficacy than under low perceived coping efficacy. This corresponds to the interaction effect described by previous research (Cismaru & Lavack, 2007; Rogers & Prentice-Dunn, 1997; Witte & Allen, 2000). However, it may be an oversimplification to conclude that individual IS security behavior may be enhanced by solely increasing information on current IS security hazards. Our simulation revealed that an externally induced increase of the perceived overall threat produced a counter-productive impact on the individual IS security behavior when the perceived coping options were low. In this case, the model behavior showed an emotion-focused response and increased the tolerated threat threshold, becoming resigned to the threat. This phenomenon has not yet been reported by other research.

Our model of individual threat control reached higher levels of individual IS security behavior under high perceived coping efficacy than under low perceived coping efficacy. This is in line with empirical studies, which found a positive correlation between components of the coping appraisal and IS security behaviors or intentions (Ng, et al., 2009; Rhee, et al., 2009; Workman, et al., 2008). However, our simulation results imply that high perceived coping efficacy is a necessary, but not sufficient, precondition for high individual IS security behavior. Simultaneously, a perceived discrepancy between the perceived current threat and desired level of threat is needed to create a change in protective behaviors. Only then was an externally induced increase in the perceived coping efficacy relevant for behavior change. This is a further phenomenon which has not been reported in the literature.

5.2. Limitations and open issues

Dynamic modeling provides a helpful tool to rigorously model complex reciprocal relationships of psychological systems. However, decisions have to be made about boundaries of the system to be explained. Thus, it has to be decided what variables will be explained endogenously by the model structure, what variables work as external impacts, and what variables are to be omitted (Hirsch, et al., 2007). Our model focused on the interactions between perceived threat and security behavior. We neglected impacts of information processing related to the appraisal of threats and coping options (e.g., investigated by Das, et al., 2003; De Hoog, et al., 2007; Meijnders, et al., 2001a; Meijnders, Midden, & Wilke, 2001b; Neuwirth, et al., 2000). We fully refrained from pos-

ing questions regarding indicators of the perception of the overall threat and also did not discuss how such indicators should be presented in order to be most effective.

The variables in the model are on a general level. Hence, the model may gain from a distinction of different elements of the perceived overall threat (severity, vulnerability) and coping efficacy (self-efficacy, response efficacy, costs), as proposed by the protection motivation theory (Liang & Xue, 2009; Rogers, 1975, 1983; Rogers & Prentice-Dunn, 1997).

Furthermore, our model ignored the impact of previously experienced hazard incidents. It can be assumed that such experiences reduce the level of goal achievement expectancies, i.e., the perceived coping efficacy (Rassmussen, et al., 2006), or affect the perception of the overall threat (Sawyer & Kernman, 1999).

A potential extension of the proposed model would be the inclusion of an external disturbance on the individual IS security behavior, i.e., the input quantity, as proposed by the perceptual control theory (Powers, 1990). Then, we would be able to model a situation in which individuals cannot implement an intended protective behavior, for example due to a temporary work overload. In such a case, an adaption of the reference value, i.e., the tolerated threat threshold, may be expected (Carver & Scheier, 1990; Rassmussen, et al., 2006; Wrosch, Scheier, Carver, et al., 2003; Wrosch, Scheier, Miller, Schulz, & Carver, 2003).

A second extension of our model might encompass an endogenous explanation of the perceived coping efficacy, as investigated by Schmidt and Dolis (2009). In their model of achievement of working task goals, they assumed the goal achievement expectation to depend on given resources (remaining time to solve the task), and on the perceived discrepancy (remaining tasks).

A third possible expansion of the model might entail a moderation of the relationship between individual IS security behavior and perceived non-covered threat by perceived coping efficacy, as it was found that individuals with high self-efficacy convictions overestimated the effectiveness of their actions. Consequently, they devoted less effort to the achievement of a work task (Vancouver & Kendall, 2006; Vancouver, et al., 2002; Vancouver, et al., 2001).

Finally, an endogenous derivation of the delays should be considered in future work.

5.3. Implications for further research

Our model builds on theoretical and empirical findings reported in the literature. However, in order to strengthen the validity of the model, further empirical work is required. Our model may guide the operationalization and measurement of variables, as well as provide a new framework for the interpretation of empirical findings. Compared with previous dynamic risk models, which remain on a verbal level, our model is sufficiently specific and mathematically defined to be tested empirically. Thus, a first step has been made towards a better establishment of dynamic models of individual IS security threats, which complement unidirectional models. The empirical

testing of our model is an important next step. Therefore, a longitudinal design with ratio-scaled data is required (Levine, 2000; Levine, et al., 1992). Such an examination might focus on the persistence of the different stock variables over time and the sizes of the different time delays, respectively. Furthermore, the form of the proposed causal relationships should be investigated. In our model of individual threat control, they were assumed to be linear. However, they may be better represented by non-linear relationships, which are moderated by changing sizes of the delays. And finally, the different ways in which people react to threatening situations (cf. the types described above) should be investigated empirically.

As an important benefit, dynamic modeling procedures may raise questions that would not have been detected by conventional unidirectional models (Levine & Doyle, 2002); an important added value of this method. In this study, such questions occurred concerning the kind and impact of principles relevant to IS security, the counter-productive effect of high-threat messages, or the preconditions for effective coping interventions, to which further scientific interest should be directed. A further specification raised by our research, from which unidirectional models may profit, is the need for a differentiation of the threat appraisal concepts. Items on perceived threat should allow previously undertaken mitigating behaviors to be controlled for. The author of the protection motivation theory was probably aware of the reciprocal impact of security behavior on perceived threat. Originally he defined the component 'vulnerability' as 'the conditional possibility that an event will occur provided that no adaptive behavior is performed or there is no modification of an existing behavioral disposition' (Rogers, 1975, p.97). However, common operationalizations of the vulnerability component do not consider previously undertaken security measures (cf. item formulations of Rippetoe & Rogers, 1987; Workman, et al., 2008). Items on perceived threat should avoid confounding the perceived current state and the desired level of risk by explicitly investigating the latter. Unfortunately, even studies adopting the risk homeostasis theory failed to measure indications on the target level of risk (e.g., Sawyer & Kernman, 1999; Simonet & Wilde, 1997).

Finally, our model of individual threat control may help to understand and reinterpret previous findings. For example, Kuttschreuter and Gutteling (2004b) investigated the development of individual risk perception and mitigating behavior regarding the millennium bug. Contrary to expectation, they found that security behavior did not increase as the turn of the millennium approached (Y2K Hype), although the perceived coping efficacy increased. Against the background of a control-theoretical framework this finding is not surprising, since the authors also report a decreasing level of perceived threat, which they ascribe to the effectiveness of a risk communication campaign re-establishing the trust in the risk-mitigating competence of official institutions.

5.4. Implications for practice

The motivation of this study was to gain insights into the formation of individual IS security behavior. Our model of individual threat control is only in its infancy and has to be further refined, as described above. However, first implications for risk management can be deduced. In contrast to previous research, the model emphasizes the importance of a balanced combination of interventions, tailored to the target individual's current risk situation. Such interventions may apply to the individual's perception of current risks, coping skills, as well as values and principles concerning IS security. IS security principles, such as privacy, integrity or confidentiality of data, may be enhanced, for example, by an explicit organizational security culture, by strengthening the user's sense of obligation and responsibility, as well as by senior managers' model behavior (Herath & Rao, 2009; Leach, 2003; Stewart, 2004). Furthermore, IS security principles can be strengthened by ruling out competing values. Thus, work surroundings should be created that take away time pressure and work overload, and methods of satisfying competing interests without offending security issues should be pointed out (Post & Kagan, 2007; Sasse, et al., 2001). Users' coping skills could be improved by repeated training fostering general knowledge in computer systems, and the applications of software and the Internet (Rhee, et al., 2009). Finally, users should repeatedly be informed about the severity and vulnerability of actual threat levels (Workman, et al., 2008). Our findings emphasize that increased coping skills may only be implemented if underlying security values are high enough to foster the need for a low tolerated threat threshold, and if this tolerated threat threshold is exceeded by the perceived threat of the actual situation. In addition, enhancing the perceived threat of the current situation may only succeed when perceived coping efficacy is high. Only then can Moore's (2003) claim to transform users from the biggest vulnerability of IS security into the first line of defense be successfully realized.

Chapter 5:
Overall Discussion and Conclusion

1. Introduction

At present, technological progress in information and communication technologies (ICT) is attaining new characteristics: ICT will increasingly be interconnected as well as integrated within commodity items, thereby ubiquitously shaping daily settings. Besides bringing about improvements, this development also harbors various risks. This thesis was guided by interest in the human dimensions regarding risks of ubiquitous ICT. The topic has been investigated with reference to three aspects: first, the subjective appraisal of risks connected with ubiquitous ICT by potentially concerned people; second, preconditions of individual protective behavior; and third, the production of risks through technological reactance or omission of security behavior. In conducting the investigation, different methodological approaches were used. In a first study (delineated in chapter 2), mental representations of risks of ubiquitous ICT were explored by means of qualitative interviews. Study 2 (presented in chapter 3) examined, using quantitative survey data, a model that related different aspects of perceived threats of ubiquitous ICT and perceived coping efficacy of protective measures to different protective and non-protective reactions. In study 3 (chapter 4), a conceptual 'model of individual threat control' was developed, explaining security behavior regarding current ICT risks. This mathematical model reflected the reciprocal relationships between individual perception of risks and mitigating reactions. The model allowed the progression of risk mitigating behavior to be simulated over time and under different initial conditions and externally manipulated impacts.

Specific research questions of the individual studies have already been discussed in the corresponding subchapters. This final chapter aims first to reconsider the findings in a comprehensive way, based on the overriding research objectives formulated in chapter 1. Then, the general procedure followed in this thesis is reconsidered, and finally, implications for future research and practice are derived.

2. Reconsidering the overall findings

The discussion of the overall findings follows the three research aspects mentioned above, i.e., risk appraisal from the viewpoint of people concerned, the preconditions of successful individual risk management, as well as of potential individual behaviors that would cause or lead to further risks involving ubiquitous ICT. The dynamic model of individual threat control, formulated in study 3, serves as a framework for integrating the various aspects, which are subsequently discussed. For ease of understanding, the main points have been visually integrated into the dynamic framework, shown in Figure 5.1.

2.1. Subjective appraisal of risks of ubiquitous ICT

To be concerned implies the perception and appraisal of threats of ubiquitous ICT. Therefore, a first objective of this thesis was to find out how risks of ubiquitous ICT are appraised by potentially concerned people. The conceptual 'model of individual threat control', as shown in Figure 5.1, distinguishes three constructs with regard to the threat appraisal process. The first is 'tolerated threat threshold', which represents a desired goal or reference value. The second construct is 'perceived overall threat'. This construct describes the perceived current level of the overall danger. And the third construct, 'perceived non-covered threat', encompasses an estimation of how much of the perceived overall threat is not covered by previously undertaken safeguarding measures. In the following, potential impacts on these three threat appraisal constructs are discussed in relation to the risks of ubiquitous ICT.

Impacts on the tolerated threat threshold

Following the model of individual threat control developed in chapter 4 and in accordance with control-theoretical frameworks (Wilde, 1982b, 1998), the tolerated threat threshold defines the risk level an individual is willing to sustain. This threshold was assumed to be the result of a balancing of security principles and principles competing with the former. So far, they have only been discussed regarding existing ICT risks (cf. section 5.1 in chapter 4). Thus, a bridge has to be built to the findings of study 1 (chapter 2) in order to learn what principles or values respondents saw as being endangered by ubiquitous ICT: study 1 explored the changes which individuals anticipate from ubiquitous ICT. It was found that the respondents feared for various personal and social principles, such as privacy, fairness, individual autonomy, social capacity, and freedom (of choice). These were seen as endangered by ubiquitous ICT, as the technologies were assumed to bring increases of external control, discrimination, surveillance, data abuse, and data defectiveness. Undermined privacy and increased discrimination are concerns that are commonly shared by experts (Beresford & Stajano, 2003; Friedermann, et al., 2006; Greenfield, 2006; Kleinhückelkotten & Neitzke, 2009; Stajano, 2003). Contrary to the experts' view (e.g., Hilty, 2005; Poldervaart, 2009; Waeger, et al., 2005), however, the respondents in study 1 lacked any awareness of ubiquitous ICT risks endangering ecological principles.

Study 1 revealed further that the impairments from ubiquitous ICT which the respondents feared by far exceeded expected benefits. Rather than being for the whole society, such benefits were seen to be restricted to individual users of the technological applications, for example in the form of gains in control and time, or monetary privileges. This predominance of anticipated negative changes probably indicates a currently low tolerated threat threshold regarding ubiquitous ICT. It might, however, be expected that the threshold will increase when the advantages of ubiquitous ICT become more salient and concrete with their increased diffusion.

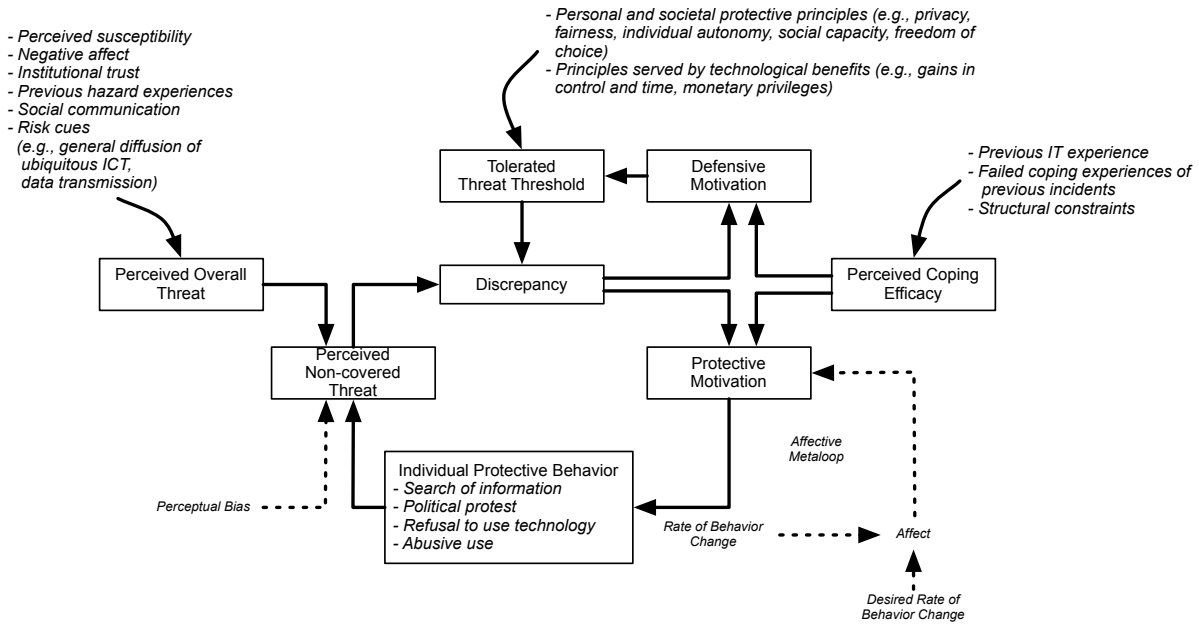


Figure 5.1. Individual control of risks of ubiquitous ICT. An integrative visualization of the overall findings.

Impacts on the perceived overall threat

The perceived overall threat of the 'model of individual threat control' corresponded to the perception of the current danger. The variable 'perceived threat', which was assessed in study 2, may be an indicator for this construct. The results of study 2 showed that the level of the perceived threat is correlated with personal susceptibility, evoked negative feelings, and a lack of trust in precautions taken by institutions. These impacts on the perceived threat have also previously been found in other risk contexts (Grothmann & Reusswig, 2006; Kuttschreuter, 2006; Siegrist, 2000; Siegrist, et al., 2000).

The study of the perception of risk is directly associated with the question of the perceptibility of the risks: As these are not directly observable with sensory perception, they have to be indirectly deduced from previous experiences, social communication or from available risk cues (Böhm, 2008; J. X. Kasperson, Kasperson, Pidgeon, & Slovic, 2003; Siegrist & Gutscher, 2006). This is particularly true for risks of ubiquitous ICT. Study 1 tried to comprehend the respondents' trains of thought, in order to understand which cues their fears were based on. We identified two main drivers of the negative changes: an increased acceptance and diffusion of ubiquitous ICT in society, as well as an increased interconnectedness of data pools due to transmission of data from one institution to the other. Both indicators may be assumed to develop continuously without noticeable advances. Such progressions are barely perceptible for individuals. Furthermore, due to the invisibility inherent in ubiquitous ICT, the increased interconnected-

ness of data files may remain hidden to individuals altogether. Thus, a main challenge for subjective perception may be that changes in the risk cues remain unnoticed.

Impact on the perceived non-covered threat

As the third construct relevant to the threat appraisal process, the 'model of individual threat control' acknowledges the perceived non-covered threat, which is the fraction of the perceived overall threat left uncovered by previously undertaken precautionary measures, and omitted risky behaviors. Following the 'model of individual threat control', this construct is affected by the perceived overall threat and by an estimation of the effectiveness of protective actions performed. What such protective actions might be will be discussed in the following section.

The 'model of individual threat control' in study 3 assumed an unbiased impact of protective behaviors on the perceived non-covered threat, based on findings on protective health behaviors (Brewer, et al., 2004; Gerrard, et al., 1996; Renner, et al., 2008). It may be, however, that the protective impact of previous protective behaviors on perceived non-covered threat will be overestimated by individuals. Such a perceptual bias, as introduced in Figure 5.1, should be the subject of further research.

2.2. Individual risk management: Preconditions for protective behavior

A second main objective of this thesis was the investigation of preconditions for protective behavior. To this end, we first had to identify what such protective behaviors might be. Second, we were interested in components impacting protective behaviors – namely, the impacts of the perceived threat, the perceived coping efficacy, and the affective reactions - as well as the precursors of these factors. Third, we were interested in potential evolutions of protective behaviors over time and under changing external impacts.

Protective behaviors against the risks of ubiquitous ICT

With the help of the qualitative interviews in study 1, we explored what the respondents meant to do in view of the anticipated threats of ubiquitous ICT. The search for information on the use of ubiquitous ICT and political activism against the implementation of ubiquitous ICT in the public sector, emerged as primary intentions. Both examples are rather unspecific behaviors; however, more concrete ideas of protective actions could not have been expected in view of the currently very abstract threats of ubiquitous ICT. Furthermore, the search for information and the political protest have previously been investigated regarding, for example, environmental threats (Homburg & Stolberg, 2006; Martens, 2007; Martens & Rost, 1998). Therefore, these two

examples were transferred to the quantitative model test of study 2 as dependent variables in the form of intentions.

The pattern that evolved from the interviews in study 1 led to the assumption that the use of ubiquitous ICT per se was seen as a risk-producing behavior. The use of these technologies was the imaginary starting point for the trains of thought which resulted in the threatened principles referred to. Thus, a refusal to use certain technologies may be an even more imminent protective reaction. Furthermore, if an externally forced participation was feared, several participants mentioned that their next reaction would be to avoid data registration through abusive behavior. The discussion will return to this point below.

Components impacting protective intentions

Both the empirical unidirectional model of study 2 and the conceptual control-theoretical model of study 3 followed propositions of the 'Protection Motivation Theory' (PMT) (Rogers, 1975, 1983). PMT states that a protective reaction can be predicted by the level of the perceived coping efficacy together with the level of the perceived threat. The correlations found in study 2 supported the assumed impacts of the perceived coping efficacies on the corresponding protective intentions. These relationships were shown to be even stronger than those between the protective intentions and the perceived threat. This predominance of the impact of the perceived coping efficacy compared with that of the perceived threat had been previously revealed by meta-analytic research (Milne, et al., 2000). The effect is not surprising considering the help of the 'model of individual threat control' of study 3. As shown in Figure 5.1, this model implies that the impact of the perceived threat on protective behavior is moderated twice – by previously undertaken security measures and by the tolerance threshold – whereas the perceived coping efficacy impacts directly on the protective intention.

Next, we were interested in precursors of the perceived threat and coping efficacy. Those relevant to the perceived threat have already been discussed above. Regarding the perceived coping efficacy, the quantitative test in study 2 revealed positive correlations between previous IT use and the perceived coping efficacy of both protective intentions tested. The impact of IT expertise is in line with previous research (Kuttschreuter & Gutteling, 2004a). However, experiences may also lessen the perceived coping efficacy, namely if they relate to failed coping with previous incidents. This relationship was unfortunately not included in the empirical work of study 2, but has been stressed theoretically (Rassmussen, et al., 2006), and shown empirically in relation to flood risks (Grothmann & Reusswig, 2006; Siegrist & Gutscher, 2006).

Clearly, a high perceived coping efficacy requires structural conditions with high degrees of freedom for individual protective actions. Respondents in study 1 were apprehensive of external

constraints, such as the lack of technology-free alternatives, and financial disadvantages, which, for example, may render the strict avoidance of ubiquitous ICT impossible.

In addition to the impacts of perceived threat and coping efficacy on protective intentions, in study 2, a motivational affective impact was assumed, based on the propositions of other researchers (De Hoog, et al., 2007; Loewenstein, et al., 2001; Peters, et al., 2006). However, the empirical model testing unexpectedly revealed the relationship between the negative affect and the protective intentions to be negative. This finding raised questions about a potential second process, that of fear control, which may become active when the control of the danger fails. Such dual process models have been described by Leventhal (Leventhal, 1970; Leventhal, et al., 1992) and Witte (Witte, 1994, 1998; Witte & Allen, 2000). These frameworks stimulated questions about the reciprocity of the processes (Wiebe & Korbel, 2003), which essentially shaped the construction of the 'model of individual threat control' in study 3.

Nevertheless, the construction of the 'model of individual threat control' refrained from including an affective construct. Control theories describe the role of affect as much more complex than the unidirectional relationships which were assumed in study 2. Carver and Scheier (1990) propose that affect is integrated in a second meta-loop system, indicated in Figure 5.1, in addition to the primary action loop. This meta-system monitors the rate of discrepancy reduction of the action loop. Its reference value is the desired rate of discrepancy reduction. A perceived reduction rate above the reference value indicates that the discrepancy will be dissolved faster than expected. Hence, positive affect is experienced, resulting in a reduction of the efforts to achieve the goal of the action loop. If the perceived rate of discrepancy reduction of the action loop falls below the desired rate, negative affect results. Consequently, goal-achieving efforts are increased (Carver, 2004). However, an override mechanism prevents efforts from being endlessly invested in unachievable goals. Thus, at a certain point, an additional increase of negative affect changes into a disengagement from the action goal. This occurs particularly in cases where the action goal is not closely tied to the self (Carver, 2006).

The conceptualization of the control-theoretical affective meta-loop seems very appealing. However, it has to be made more concrete before translation into a mathematical model can be considered, and the proposed core model of individual threat control should be better consolidated before extending it with further loops.

Evolvement of the protective behavior level over time and under changing external impacts

Unidirectional models, such as the one tested in study 2, try to explain or predict intentions or behaviors at a certain point in time. In contrast, the dynamic 'model of individual threat control' of study 3 proposes that over a longer time horizon, individuals seek compatibility among their perception, their behavior, and their internal values. From a psychological point of view, the

assumption of an internal balance is not new, but can already be found, for example, in the work of Festinger (1957).

To achieve a behavior change, the internal balance has to be disturbed. Within fear appeal theories, such as the PMT, this is attempted by providing threat-arousing information. In relation to a procedural evolvement over time, however, it must be asked how long the impacts of such appeals may hold on. Furthermore, the impact of such threat appeals may be constricted by structural restrictions of the degrees of freedom (which are reflected in the perceived coping efficacy), and the individual's competing needs (which raise the tolerated threat threshold). As was visualized by the model simulation in study 3, there may be a danger that repeated threat information blunts individuals' reactions and fosters indifference and resignation. Thus, from a process-theoretical point of view, threat appeals should be preceded by an increase in the valuation of protective principles. With regard to ubiquitous ICT, these may, for example, be privacy or social fairness. Moreover, perceived opportunities for protective behaviors have to be fostered, before delivering threat information.

A gradual evolution of protective behaviors over time has been postulated by stage models, such as the 'transtheoretical model of behavior change' (TTM) of Prochaska and colleagues (Prochaska & DiClemente, 1986; Prochaska, DiClemente, & Norcross, 1992; Prochaska, Norcross, & DiClemente, 2006; Prochaska & Velicer, 1997). The TTM describes five stages through which an individual has to pass in order to achieve a high level of protective behaviors. These stages range from a complete unawareness of the threats in the first stage, to a stable maintenance of the protective behaviors in the final stage. Empirically, it was shown that the number of principles an individual holds against the protective behaviors decreases over the five stages, whereas the number of principles in favor of the protective behaviors increases. The pro-principles normally start to outweigh the cons in the second phase, the 'contemplation' stage, in which the individual develops the need for a behavior change (Hall & Rossi, 2008; Prochaska, et al., 1994; Velicer, Norman, Fava, & Prochaska, 1999). The changing rate of the pro and con principles may be an indication of a decreasing threat tolerance level. Thus, a combination of the 'model of individual threat control' with stage models, such as the TTM, may be promising.

2.3. Risk of ubiquitous ICT emerging from individual behavior

A final objective of this thesis was to find indications of how individual behavior may cause risks of ubiquitous ICT. The main interest was directed at conditions fostering technological reactance and the omission of protective behaviors.

The emergence of technological reactance

Based on Mehrabian and Russell (1974), Spiekermann and Rothensee (2005) have described a model to explain reactance to ubiquitous ICT. These authors assumed that reactance, i.e., the avoidance of and work against the technologies, is aroused by a perceived withdrawal of control. The authors mention this loss of control to be inherent to ubiquitous ICT, since the decisions for their implementation are mostly not made with individual consent, and technology-free alternatives are not available. The goal of technological reactance is to recuperate endangered freedoms (Brehm & Brehm, 1981; Spiekermann & Rothensee, 2005). These assumptions correspond exactly to the findings of study 1. Our respondents first mentioned their intention to renounce the use of ubiquitous ICT. However, they admitted that external constraints, such as the lack of technology-free alternatives, may force the adoption of applications based on ubiquitous ICT. In this case, the respondents considered abusive reactions such as boycott, manipulation, and incorrect or minimal use. Such behavior may reduce the overall usefulness of ubiquitous ICT and create risks of data defectiveness or the criminalization of citizens.

Omission of protective behavior and its evolution over time

The omission of protective behaviors may have two causes: it may occur, first, if no appreciable threat is perceived, and second if an individual is worried, but does not see any options for protection (Rippetoe & Rogers, 1987; Witte & Allen, 2000). In the latter case, the individual engages in non-protective reactions, in the form of feelings of helplessness, overstrain, or by denying the threat or their own involvement. The model test in study 2 revealed that in addition to a high perceived threat and low perceived coping efficacy, such non-protective reactions correlated positively with negative affect. Following Witte (1994, 1998), in this case, the individual tries to control his or her fear. Within the 'model of individual threat control' of study 3, this assumption was adapted by assuming that non-protective reactions lower protective principles. This is a development, which unfortunately could not have been investigated empirically by the cross-sectional design of study 2. The consequence of lowering protective principles and values was described above; individuals may become indifferent about the risks. Following the 'model of individual threat control', the interruption of this pattern may only succeed if risk communication is combined with highlighting protective values and providing concrete options for protective behavior.

As initially mentioned, the omission of protective behavior may also be rooted in a failure to perceive current threats. As the simulation in study 3 revealed, such a situation may not only be due to the absence of perceivable threat information, but also to individual estimation that protective principles are lower than competing principles which evolves from the benefits brought

about by the use of the technologies. Also in this case, threat appeals may be more effective if combined with addressing the maladjustment of the principles.

3. Reconsidering the general procedure

The work for this thesis has broken new ground in psychological science, bringing with it several uncertainties. First of all, the object of the research – the risks of ubiquitous ICT – was very abstract and future-oriented. At least at the beginning of the work, concrete technological examples were elusive. Second, the 'cognitive mapping' method used in study 1 and the 'system-dynamics' modeling in study 3, were two rather innovative methodological procedures in psychological research. Thus, their adaptation to psychological research questions required considerable effort. The experiences gained with the concrete implementation of the work allowed several weaknesses to be identified in the procedure chosen, which should be avoided in future research with similar research designs.

The three individual studies, which differed completely in methodological terms, highlighted different aspects of the human dimensions of the risks of ubiquitous ICT, as discussed in the preceding sections. These complementary perspectives are an inherent gain of methodological triangulation (Flick, 2004). However, the individual studies were also meant to build on each other, as was introduced in chapter 1 (section 6). They would have benefited even more from each other if their options and limitations had been known from the outset. In the following, these options and limitations as well as demands which were raised regarding the overall procedure will be reconsidered.

3.1. Elicitation of mental risk representations with the cognitive mapping method

Cognitive interview techniques to elicit mental models are suitable for gaining first information in a loosely structured domain, since these methods are straightforward and systematic, and yield relatively complex and consistent representations of the individual subjective models (Langan-Fox, et al., 2000). These strengths were supported by the procedure in study 1: the interviews generated a richness of data in a relatively short time, which would have hardly been reached with other qualitative techniques. The visual feedback provided during the interviews motivated the respondents to interconnect and continue their trains of thought and also demanded consistent statements.

However, the method places high demands on the interviewer and the resulting findings may be shaped by his or her skills and background (S. M. Brown, 1992; Langan-Fox, et al., 2000). During the interview, the interviewer has a dual task. He or she has to guide the interview, and simultaneously to visually depict the statements of the respondents. This depiction demands a first ab-

straction of the statements, which therefore already has to be done during the interview. These problems were countered with various 'test' interviews prior to the 'real' interviews, in order to increase the interviewer skills of the author of this thesis.

Brown (1992) criticized the low interviewer reliability of the method. This is of minor importance to this thesis, since all interviews were conducted by the same person. The restriction to one interviewer, however, may, on the other hand, have augmented the danger of an interviewer bias. Brown further emphasized a low retest reliability, since effects of learning and remembering, as well as temporal associations, may bias the evolving maps. In this sense, cognitive maps represent 'vivid snapshots' without claims to generalization. These weaknesses of the method can be accepted when considering the main purpose of the qualitative exploration in study 1: the identification of first insights into representations of ubiquitous ICT, meant to be fruitful for the subsequent research steps.

This (undemanding) goal, and the richness of data produced in each interview, legitimated the low number of interviews (Morse, 2000) that were conducted. However, it should be acknowledged that the choice of respondents was not guided by a classical theoretical sampling (Strauss, 1999), and that the number of interviews was determined by the time schedule of the project rather than by construct saturation. Furthermore, it cannot be excluded that the input material used biased the statements of the respondents. It is probable that the example used of ubiquitous ICT applications in the outpatient health sector failed to elicit, for example, any ecological associations. The nature of the input material may further be the reason why the interviewees perceived only few improvements from ubiquitous ICT, and these only for individual users rather than for the whole of society.

Retrospectively, it can be stated that the exploration in study 1 delivered a good basis, in the form of key concepts and contents for the item formulation, for the subsequent quantitative test in study 2. The cognitive maps failed, however, to provide structural insights suitable for transformation into the dynamic model of study 3, a procedure that has been proposed by Howick and colleagues (Howick, Ackermann, & Andersen, 2006; Howick, Eden, Ackermann, & Williams, 2006). From a psychological point of view, the validity of subjective representations for reconstructing objective (psychological) systems must be questioned (Doyle & Ford, 1998). Hence, the preference was to base the dynamic modeling in study 3 on theoretical foundations rather than on the structural representations elicited in study 1.

3.2. Testing a structural equation model to explain protective and non-protective behavior

The limitations of the quantitative model test have already been discussed in detail in chapter 3. Thus, in the following, only the main points will be summarized.

The large sample, as well as its representative selection by the ADM master-sampling method (Behrens & Löffler, 1999), allowed for a broad generalization of the results to the inhabitants of Germany, and similar results might be expected from comparable countries such as Switzerland or Austria.

The cross-sectional design of the survey in study 2 allows only for assumptions on correlations. Questions on causality or reciprocity cannot be addressed with this design. In particular, an empirical foundation for the dynamic model in study 3 would have required longitudinal data.

Finally, it should be remembered that the items used were formulated especially for the purpose of this survey, as reliable measurement instruments for the subjective appraisal of the risks of ubiquitous ICT did not yet exist. Furthermore, due to the diverging particular interest of the research partners involved, the space in the questionnaire was limited and did not allow for the inclusion of large item scales.

3.3. Conceptualization of the model of individual threat control with the system-dynamics methodology

Computational simulation models are particularly suited to integrating divergent theories and empirical findings. Such an integration fosters a deeper theoretical understanding (Levine & Doyle, 2002; Tobias & Mosler, 2007). To allow for the mathematical specification of the model's contents, theoretical and empirical assumptions have to be more precise and explicit than a mere verbal formulation would demand. Thus, system-dynamics modeling can support integrative theory building, and increases the falsifiability of the underlying assumptions, as well as their coherence and consistency (Levine & Doyle, 2002; Schwaninger & Groesser, 2008; Schwaninger & Pérez Rios, 2008). These were precisely the purposes for which the modeling was used in this thesis. With the help of computational modeling, different (competing) control-theoretical and unidirectional approaches explaining protective behavior were included in an integrative model.

Although computational modeling supports the integrative procedure, such an integration was rather challenging, as the author of this thesis experienced several times during the implementation. The difficulties regarding the usefulness of the qualitative visual risk representations, elicited in study 1, were mentioned above. However, an integration of the findings from the quantitative model test in study 2 was also challenging. The main problem here is related to the divergent basic structural units upon which the different methodological approaches focus: unidirectional models, such as that in study 2, are interested in the strength of single relationships between variables, whereas the basic unit of system-dynamic modeling is a closed reciprocal feedback loop between two or more variables (Hirsch, et al., 2007; Levine, 2000). The strengths of the single links are of minor interest, since cross-sectional investigations may not guarantee the

stability of the findings over time. Therefore, their empirical validation would require time series of data, rather than assumptions on strengths of the relationships.

A further aspect that must be considered when building computer models is the rather high expenditure of time needed for training in the method, and the implementation of a model (Hirsch, et al., 2007; Tobias & Mosler, 2007). Within the framework of this thesis, a conceptual model, based on the literature, was worked out. An empirical test of this model would have gone beyond the scope of this thesis. However, an empirical test is the next imperative step for the further development of the proposed 'model of individual threat control', from which its validity may strongly benefit.

For both the research project, in which this thesis was embedded, and for the thesis itself, the construction of a dynamic model was not the overall objective, but merely a further discrete research step, equivalent to the studies 1 and 2. The procedure of this work was determined by the schedule of the overall research project. For future planning of research, it should be considered, however, whether the procedure should be better aligned to the elaboration of the dynamic model. In that case, a more classical procedure should be aspired to (as, for example, described by Hirsch, et al., 2007; Levine, et al., 1992; Schwaninger & Groesser, 2008; Tobias & Mosler, 2007), by developing first a theoretical conceptual model, followed by empirical work for its validation.

4. Implications of the overall findings

From the considerations outlined so far, several implications can be drawn for further research and practice.

4.1. Implications for further research

Within this thesis, qualitative, quantitative, and conceptual foundations have been elaborated in order to consider different human dimensions of the risks of ubiquitous ICT. During the five years work on the thesis, the principle of Moore (1965) continued to hold true and technological progress continued to accelerate dramatically. First technological applications based on ubiquitous ICT have been released and diffused (such as shopping by Internet, multifunctional mobile phones, electronic passports, and electronic patient cards), or stand ready to break through (e.g., logistics in supermarkets and libraries based on RFID tags and smart ammeters). Subsequent research with regard to risks of ubiquitous ICT may benefit from the concrete examples available. Thus, the abstract level, to which the present research was limited, can be avoided in future. Furthermore, future research may have the opportunity to accompany the implementation

and diffusion of concrete technological applications with longitudinal monitoring. In so doing, particular interest should be devoted to the following research questions:

- What personal and societal principles do ubiquitous ICT applications satisfy? And with what protective principles are these incompatible?
- Based on what cues can risks of ubiquitous ICT be perceived (such as media news, hazard experiences, changes in the environment with signal function)? How could such cues be directly integrated into the technological settings (e.g., in the form of automatized warnings)? How should such cues be shaped in order to be effective? How long does the effect of such cues persist?
- What individual response patterns causing or mitigating risks do users develop in relation to ubiquitous ICT applications? What capabilities or skills may be lost? To what behaviors might users attribute protective effectiveness, even though, seen objectively, these have no objective impact on risk mitigation?
- What emotions are related to ubiquitous ICT applications, and how do they shape the individual response patterns?
- How might the current individual prerequisites for actions and decisions be restricted by ubiquitous ICT? Do such structural restrictions yield to a perceived loss of control? And how could this be prevented?
- Does perceived technological dominance and loss of control produce technological reactance? Can such adverse reactions cause societal risks?
- Do perceived loss of control and low perceived coping efficacy foster reactions such as disengagement in protective principles, resignation, a disregard of risk cues, or the omission of even simple protective measures?

From a conceptual point of view, within this thesis, a dynamic model has been elaborated which substantiated control-theoretical verbal propositions into a mathematical computer-based working model. This model has the potential to stimulate psychological risk research beyond a mere theoretical and technological context. Three main implications can be derived for further empirical risk research:

First, the measurement of threat appraisal should differentiate among statements covering an overall perception of the danger (the perceived overall threat), statements about the importance devoted to the threatened values (predicting the tolerated threat threshold), and statements on judgment of the level of threat after consideration of previous protective behavior (the level of the non-covered threat). It must be admitted that the operationalization of these constructs may be challenging, since a high level of confounding has to be expected.

Second, following the dynamic model, careful attention should be paid to the impact of previous protective behavior on the perceived non-covered threat, and a behavior change should be understood as an increase in the current level. This requires controlling for the current level of protective behavior.

Third, psychological risk research should devote effort to the implementation of longitudinal designs. Such designs could be oriented towards 'naturally' occurring incidents. For example, Kuttschreuter and Gutteling (2004b), or Sawyers and Kerman (1999) tried to capture events such as the Y2K hype on the turn of the millennium, and the releasing time of a defective software. Another option may be presented by laboratory experiments, manipulating information on the current danger, coping options, or framing principles. Control-theoretical experimental designs in relation to working goals have been implemented by Vancouver and colleagues (Vancouver, et al., 2005), Schmidt and Dolis (2009) or Tolli (2009).

From a methodological point of view, within this thesis, two new methodological approaches have been adapted for risk psychological research questions. Advantages and pitfalls of their implementation have been presented above. In particular, the method of computer simulation has been claimed to be a useful approach for research on complex psychological systems (Hirsch, et al., 2007; Tobias & Mosler, 2007). It is probable that this thesis may ease the way for other researchers to try these new methodological approaches.

4.2. Implications for practice

Based on the individual studies of this thesis, different propositions for practice were formulated in the corresponding subchapters. In particular, those in the chapters 3 and 4 concern recommendations for the design of risk information campaigns. At this point, the scope will be expanded by addressing further stakeholders. The following recommendations have been arranged with regard to preservation of individual control, encouragement of trust in the technologies, and prevention of individual technological overstrain. Questions concerning prevention of the ecological, economic or health risks of ubiquitous ICT are not of minor importance, but less inherent to the work of this thesis and therefore not covered here.

Implications for designers of ubiquitous ICT: For designers, questions about technical standards and issues of data security may have priority. Thus, there is a danger of the individual user's perspective becoming lost. As our project partners estimate, 30% of people feel overstrained by ubiquitous ICT (Kleinhückelkotten & Neitzke, 2009). Despite the high prevalence of ICT, IT literacy in the population should not be overestimated. The design of ubiquitous ICT applications should thus focus on intuitive usability and utility, and refrain from providing overwhelming additional services. In addition to the 30% of overstrained people, 37% of people hold

a rather skeptical attitude towards ubiquitous ICT (Kleinhückelkotten & Neitzke, 2009). These people have a right to decide against using the technologies. This is only possible if, first, the implementation of technological solutions is transparently perceivable, and second, there is always the chance to opt out of the technology. Thus, ubiquitous ICT applications have to be self-disclosing and deniable (Greenfield, 2006). To ensure the implementation of these requirements, representatives of the population should already participate during the product development stage (Carius & Renn, 2003; Pidgeon & Rogers-Hayden, 2007).

Implications for companies and (public) institutions adopting ubiquitous ICT: It also holds true for these stakeholders that awareness should be directed towards the viewpoint of the individual customers. Prime importance should be given to three topics which coincide with recommendations of Meier (2005, 2006). First, the usefulness of the technological service or application should be apparent for customers. Second, protection of customers' privacy and data should receive highest priority. This is accomplished by using data restrictively and transparently, as well as by interconnecting or transmitting data only with customers' consent. Third, discrimination against people who are unwilling or unable to use ubiquitous ICT should be counteracted. Thus, services alternatively have to remain accessible in 'traditional' ways, such as from person to person or by post or telephone. Commitment to these recommendations may be essential for survival, since they strengthen customers' trust in the technological services and counteract adverse responses.

Implications for regulators: Based on the work of this thesis, recommendations from others (Bundesamt für Sicherheit der Informationstechnik, 2004; Hilty, et al., 2003; Neitzke & Vedder, 2010) can be supported entirely. Legislation should proactively create a frame for ubiquitous ICT applications. In particular, standards for the protection of privacy and data security should be released, as well as responsibilities clarified by adapting liability standards.

Implications for individual users and non-users: In order to prevent risks of ubiquitous ICT, individuals have to become 'risk managers', i.e., they have to handle the technologies competently and in a self-determined manner (Kruse, 1981). They should be critical and informed consumers, carefully deciding on the technologies they want to use, acquiring needed skills, and resisting the temptation to shift full responsibility to the technologies. There have been repeated claims for public discussions regarding what direction technological development should take, and regarding what our future everyday lives should look like (Kleinhückelkotten & Neitzke, 2009; Neitzke, et al., 2008). However, such a discourse will only develop if many people are willing to actively participate and engage proactively in current technological developments.

5. Conclusion

Visions of ubiquitous ICT settings may sound utopian, but technological progress in this direction is a reality, and its abandonment is merely wishful thinking from some parts of the population. Even more important is therefore the stimulation of public discourse on which of the technological possibilities should be implemented and which not. In particular, technological implementations in the public sector should be subject to a democratic procedure, such as was the case of the referendum on the introduction of the biometric passport in Switzerland in 2009.

A no more visionary option may be the establishment of technology-free zones, in which people are safe from annoyances through the presence of ubiquitous ICT (Hilty, et al., 2003). First steps in this direction, such as the existing banning of mobile phones in schools, or the blocking of the Webpage 'Facebook' by several employers, may indicate the need for an increased negotiation of such technology-free zones in the future. The challenge will be to find an optimal balance between human self-determination and sovereignty of control on the one hand, and technological assistance on the other, in order for the advantages of ubiquitous ICT to be unrolled, and for their risks to be preventively counteracted. Or, in the words of Greenfield: 'We must see that everyware [sic: expression Greenfield used for 'ubiquitous ICT'] serves us, and when it does not, we must be afforded the ability to shut it down. Even in the unlikely event that every detail of its implementation is handled perfectly and in a manner consistent with our highest ambitions, a paradise without choice is no paradise at all' (Greenfield, 2006, p. 247).

References

Abowd, G. D., & Mynatt, E. D. (2000). Charting past, present, and future research in ubiquitous computing. *ACM Transactions on Computer-Human Interaction, 7*(1), 29-58.

Ahern, D. K. (2007). Challenges and opportunities of ehealth research. *American Journal of Preventive Medicine, 32*(5), 75-82.

Andreassen, H. K., Trondsen, M., Kummervold, P. E., Gammon, D., & Hjortdahl, P. (2006). Patients who use e-mediated communication with their doctor: New constructions of trust in the patient-doctor relationship. *Qualitative Health Research, 16*(2), 238-248.

Armitage, C. J., & Conner, M. (2001). Efficacy of the theory of planned behaviour: A meta-analytic review. *British Journal of Social Psychology, 40*, 471-499.

Ashby, R. W. (1956). *Introduction to cybernetics*. London: Chapman & Hall.

Atienza, A. A., Hesse, B. W., Baker, T. B., Abrams, D. B., Rimer, B. K., Croyle, R. T., et al. (2007). Critical issues in ehealth research. *American Journal of Preventive Medicine, 32*(5), 71-74.

Bagozzi, R. P., & Edwards, J. R. (1998). A general approach for representing constructs in organzational research. *Organizational Research Methods, 27*, 49-87.

Bannister, D., & Fransella, F. (1980). *Inquiring man: the psychology of personal constructs*. Harmondsworth: Penguin Books.

Beaudry, A., & Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptation. *MIS Quarterly, 29*(3), 493-524.

Behrendt, D., Kleinhückelkotten, S., Neitzke, H.-P., & Wegner, E. (2007). *Identifizierung und Bewertung der Risiken ubiquitärer Informations- und Kommunikationstechnologien (AACC) durch Experten und informierte Laien [Identification and assessment of risks of ubiquitous information and communication technologies by experts and informed laypersons]*. Hanover: ECOLOG.

Behrens, K., & Löffler, U. (1999). Aufbau des ADM-Stichproben-Systems [Design of the ADM sampling system]. In ADM-Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute (Ed.), *Stichproben-Verfahren in der Umfrageforschung eine Darstellung für die Praxis* (pp. 69-91). Opladen: Leske + Budrich.

Beresford, A. R., & Stajano, F. (2003). Location privacy in pervasive computing. *Pervasive Computing, January - March*, 46-55.

BFS. (2010). Informationsgesellschaft - Indikatoren. Haushalte und Bevölkerung - IKT-Ausstattung [Information society - indicators. Households and population - ICT equipment]. Retrieved April, 9, 2010, from www.bfs.admin.ch/bfs/portal/de/index/themen/16/04/key/approche_globale.indicator.30103.301.html?open=308,2#2

Block, L. G., & Keller, P. A. (1998). Beyond protection motivation: An integrative theory of health appeals. *Journal of Applied Social Psychology, 28*(17), 1584-1608.

Böhm, G. (2003). Emotional reactions to environmental risks: consequentialist versus ethical evaluation. *Journal of Environmental Psychology, 23*, 199-212.

Böhm, G. (2008). Wahrnehmung und Bewertung von Umweltrisiken [Perception and appraisal of environmental risks]. In E.-D. Lantermann & V. Linneweber (Eds.), *Enzyklopädie der Psychologie. Grundlagen, Paradigmen und Methoden der Umweltpsychologie* (pp. 501-534). Göttingen: Hogrefe.

Böhm, G., & Pfister, H.-R. (2000). Action tendencies and characteristics of environmental risks. *Acta Psychologica, 104*, 317-337.

Böhm, G., & Pfister, H.-R. (2001). Mental representation of global environmental risks. In G. Böhm, J. Nerb, T. McDaniels & H. Spada (Eds.), *Environmental Risks: Perception, Evaluation and Management* (pp. 1-30). Amsterdam: JAI.

Bollen, K. A., & Long, S. J. (1993). *Testing structural equation models*. Newbury Park, CA: Sage Publications.

Bostrom, A., & Fischhoff, B. (2001). Communicating health risks of global climate change. In G. Böhm, J. Nerb, T. McDaniels & H. Spada (Eds.), *Environmental risks: Perception, evaluation and management* (pp. 31-55). Amsterdam: JAI.

Bostrom, A., Morgan, M. G., Fischhoff, B., & Read, D. (1994). What do people know about global climate change? 1. Mental models. *Risk Analysis, 14*(6), 959-970.

Brehm, S. S., & Brehm, J. W. (1981). *Psychological reactance: A theory of freedom and control*. New York: Academic Press.

Brewer, N. T., Weinstein, N. D., Cuite, C. L., & Herrington, J. E. (2004). Risk perceptions and their relation to risk behavior. *Annals of Behavioral Medicine, 27*(2), 125-130.

Brown, S., Hine, N., Sixsmith, A., & Garner, P. (2004). Care in the community. *BT Technology Journal, 22*(3), 56-64.

Brown, S. M. (1992). Cognitive mapping and repertory grids for survey research: Some comparative observations. *Management Studies, 29*(3), 287-307.

Bryne, M. B. (2001). *Structural equation modeling with AMOS. Basic concepts, applications, and programmings*. Hillsdale New Jersey: Lawrence Erlbaum Associates.

Bryson, J. M., Ackermann, F., Eden, C., & Finn, C. B. (2004). *Visible thinking. Unlocking causal mapping for practical business results*. Chichester: John Wiley & Sons Ltd.

BSI. (2006). *Pervasive Computing: Entwicklungen und Auswirkungen [Pervasive Computing: Trends and impacts]*. Ingelheim: SecuMedia.

Bundesamt für Sicherheit der Informationstechnik. (2004). *Risiken und Chancen der Einsatzes von RFID-Systemen [Risks and opportunities of the implementation of RFID-systems]*. Bonn: Bundesamt für Sicherheit von Informationstechnik.

Cameron, L. D. (2003). Anxiety, cognition, and responses to health threats. In L. D. Cameron & H. Leventhal (Eds.), *The Self-Regulation of Health and Illness Behavior* (pp. 157-183). London: Routledge.

Carey, T. A. (2008). Perceptual control theory and the method of levels: Further contributions to a transdiagnostic perspective. *International Journal of Cognitive Therapy, 1*(3), 237-255.

Carius, R., & Renn, O. (2003). Partizipative Risikokommunikation. Wege zu einer risikomündigen Gesellschaft [Participative risk communication. Ways towards a society responsible of risks]. *Bundesgesundheitsblatt - Gesundheitsforschung - Gesundheitsschutz, 46*(7), 578-585.

Carver, C. S. (2004). Negative affects deriving from the behavioral approach system. *Emotion, 4*(1), 3-22.

Carver, C. S. (2006). Approach, avoidance, and the self-regulation of affect and action. *Motivation and Emotion, 30*(2), 105-110.

Carver, C. S., & Scheier, M. F. (1982). Control theory: A useful conceptual framework for personality-social, clinical and health psychology. *Psychological Bulletin, 92*(1), 111-135.

Carver, C. S., & Scheier, M. F. (1990). Origins and functions of positive and negative affect: A control-process view. *Psychological Review, 97*(1), 19-35.

Carver, C. S., & White, T. L. (1994). Behavioral inhibition, behavioral activation, and affective responses to impeding reward and punishment: The BIS/BAS scales. *Journal of Personality and Social Psychology, 67*(2), 319-333.

Cismaru, M., & Lavack, A. M. (2007). Interaction effects and combinatiorial rules governing protection motivation theory variables: A new model. *Marketing Theory, 7*(3), 249-270.

Cismaru, M., Lavack, A. M., Hadjistavropoulos, H., & Dorsch, K. D. (2008). Understanding health behavior: An integrated model for social marketers. *Social Marketing Quarterly, 14*(2), 2-32.

Cole, G. A., & Withey, S. B. (1982). The risk of aggregation. *Risk Analysis, 2*(4), 243-247.

Coroama, V., & Höckl, N. (2004, April). *Pervasive insurance markets and their consequences.* Paper presented at the First International Workshop on Sustainable Pervasive Computing, Vienna, Austria.

Curry, S. J. (2007). Ehealth research and healthcare delivery: Beyond intervention effectiveness. *American Journal of Preventive Medicine, 32*(5), 127-130.

Czaijka, S., & Mohr, S. (2008). Informations- und Kommunikationstechnologien in privaten Haushalten. Ergebnisse der Erhebung 2007 [Information and communication technologies in private households. Results from the survey in 2007]. *Wirtschaft & Statistik, 9/2008*, 764-771.

Das, E. H. H. J., deWit, J. B. F., & Stroebe, W. (2003). Fear appeals motivate acceptance of action recommendations: Evidence for a positive bias in the processing of persuasive messages. *Personality and Social Psychology Bulletin, 29*(5), 650-664.

De Hoog, N., Stroebe, W., & De Wit, J. B. F. (2007). The impact of vulnerability to and severity of a health risk on processing and acceptance of fear-arousing communications: A meta-analysis. *Review of General Psychology, 11*(3), 258-285.

Dengler, S., Awad, A., & Dessler, F. (2007). Sensor/actuator networks in smart homes for supporting elderly and handicapped people. *Proceedings of the 21st International Conference on Advanced Information Networking and Applications* (pp. 863-868). Niagara Falls, Canada

Doyle, J. K., & Ford, D. N. (1998). Mental models concepts for system dynamics research. *System Dynamics Review, 14*(1), 3-29.

Drevin, L., Kruger, H. A., & Steyn, T. (2007). Value-focused assessment of ICT security awareness in an academic environment. *Computers and Security, 26*(1), 36-43.

Eagly, A. H., & Chaiken, S. (1993). *The psychology of attitudes*. Fort Worth: Harcourt Brace Jovanovich College Publishers.

Earle, T. C., & Cvetkovich, G. (1995). *Social trust: Toward a cosmopolitan society*. Westport: Praeger.

Eden, C. (1992). On the nature of cognitive maps. *Journal of Management Studies, 29*(3), 261-265.

Eden, C., & Ackermann, F. (1992). The analysis of cause maps. *Journal of Management Studies, 29*(3), 309-324.

Eden, C., & Ackermann, F. (1998). Analyzing and comparing idiographic causal maps. In C. Eden & J.-C. Spender (Eds.), *Managerial and Organizational Cognition: Theory, Methods and Research* (pp. 192-209). London: Sage Publications.

Eden, C., & Ackermann, F. (2004). *Making strategy: The journey of strategic management*. London: Sage Publications.

Edwards, J. R. (1992). A cybernetic theory of stress, coping, and well-being in organizations. *Academy of Management Review, 17*(2), 238-274.

Elliot, A. J., & Covington, M. V. (2001). Approach and avoidance motivation. *Educational Psychology Review, 13*(2), 73-92.

Eng, T. R. (2004). Population health technologies: Emerging innovations for the health of the public. *American Journal of Preventive Medicine, 26*(3), 237-242.

Eng, T. R., Gustafson, D. H., Henderson, J., Jimison, H., & Patrick, K. (1999). Introduction to evaluation of interactive health communication applications. *American Journal of Preventive Medicine, 16*(1), 10-15.

Evans, L. (1986). Comments on Wilde's notes on 'Risk homeostasis theory and traffic accident data'. *Risk Analysis, 6*(1), 103-107.

Evers, K. E., Prochaska, J. O., Driskell, M. M., Cummins, C. O., & Velicer, W. F. (2003). Strengths and weaknesses of health behavior change programs on the Internet. *Journal of Health Psychology, 8*(1), 63-70.

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford: University of California Press.

Flick, U. (2004). *Qualitative Sozialforschung. Eine Einführung [Qualitative social research. An introduction]*. Reinbek bei Hamburg: Rowohlts.

Floyd, D. L., & Prentice-Dunn, S. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

Fogg, B. J. (2003). *Persuasive technology: Using computers to change what we think and do*. San Francisco: Morgan Kaufmann Publisher.

Ford, A. (1990). Estimating the impact of efficiency standards on the uncertainty of the northwest electric system. *Operation Research, 38*(4).

Ford, A. (1999). Modeling the environment *An introduction to system dynamics models of environmental systems*. Washington DC: Island Press.

Forrester, J. W. (1961). *Industrial Dynamics*. Cambridge, MA: MIT Press.

Forrester, J. W. (1969). *Urban dynamics*. Cambridge, MA: MIT Press.

Forschungsverbund AACCrisk. (2008). Kooperative Bewertung und Kommunikation der systemischen Risiken ubiquitärer Informations- und Kommunikationstechnologien [Cooperative assessment and communication of systemic risks of ubiquitous information and communication technologies]. In M. W. Schmied & M. Wächter (Eds.), *Statusberichte zum Förderschwerpunkt „Strategien zum Umgang mit systemischen Risiken"* (pp. 31-37). Bonn: BMBF.

Frewer, L. J. (2001). Environmental risk, public trust and perceived exclusion from risk management. In G. Böhm, J. Nerb, T. McDaniels & H. Spada (Eds.), *Environmental Risks: Perception, Evaluation and Management* (Vol. Research in Social Problems and Public Policy, pp. 221-248). Amsterdam: JAI.

Frewer, L. J. (2003). Trust, transparency, and social context: Implications for social amplification of risk. In N. Pidgeon, R. E. Kasperson & P. Slovic (Eds.), *The Social Amplification of Risk* (pp. 123-137). Cambridge: University Press.

Friedermann, M., Vildjiounaite, E., Punie, Y., & Wright, D. (2006). The brave new world of ambient intelligence: An analysis of scenarios regarding privacy, identity, and security issues. *Lecture Notes in Computer Science, 3934*, 119-133.

Gardner, G. T., & Stern, P. C. (1996). *Environmental problems and human behavior*. Boston, MA: Allyn and Bacon.

Garson, G. D. (2009). Syllabus for PA 765: Quantitative Research in Public Administration, Section Reliability Analysis. Retrieved April 6, 2010, from http://faculty.chass.ncsu.edu/garson/PA765/reliab.htm

Gentner, D., & Stevens, A. L. (1983). *Mental models*. London: Lawrence Erlbaum.

Gerrard, M., Gibbons, F. X., & Bushman, B. J. (1996). Relation between perceived vulnerability to HIV and precautionary sexual behavior. *Psychological Bulletin, 119*(3), 390-409.

Glasgow, R. E. (2007). Ehealth evaluation and dissemination research. *American Journal of Preventive Medicine, 32*(5), 119-126.

Greenfield, A. (2006). *Everyware. The dawning age of ubiquitous computing.* Berkley: New Riders.

Grothmann, T., & Reusswig, F. (2006). People at risk of flooding: Why some residents take precautionary action while others do not. *Natural Hazards, 38*(1-2), 101-120.

Günther, A. (1998). Vernunft, Moral und Ökologie. Einführung in die Risikoforschung [Rationality, moral and ecology. Introduction into risk research]. In A. Günther, R. Haubl, P. Meyer & M. Stengel (Eds.), *Sozialwissenschaftliche Ökologie: Eine Einführung* (pp. 135-217). Berlin: Springer.

Hall, K. L., & Rossi, J. S. (2008). Meta-analytic examination of the strong and weak principles across 48 health behaviors. *Preventive Medicine, 46*, 266-274.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herrtwich, R. G. (2003). Fahrzeuge am Netz [Cars on the net]. In F. Mattern (Ed.), *Total vernetzt, Szenarien einer informatisierten Welt* (pp. 63-82). Berlin: Springer.

Hilty, L. (2005). Electronic waste - an emerging risk? *Environmental Impact Assessment Review, 25*(5), 431-435.

Hilty, L., Arnfalk, P., Erdmann, L., Goodman, J., Lehman, M., & Waeger, P. A. (2006). The relevance of information and communiction technologies for environmental sustainablitly - A prospective simulation study. *Environmental Modelling and Software, 21*, 1618-1629.

Hilty, L., Bruinink, A., Köhler, A., & Som, C. (2003). *Das Vorsorgeprinzip in der Informationsgesellschaft: Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt [The precautionary principle for the information society: impacts of pervasive computing on health and environment]*. Bern: TA-SWISS.

Hilty, L., Som, C., & Köhler, A. (2004). Assessing the human, social, and environmental risks of pervasive computing. *Human and Ecological Risk Assessment: An International Journal, 10*(5), 853-874.

Hirsch, G. B., Levine, R. L., & Miller, R. L. (2007). Using system dynamics modeling to understand the impact of social change initiatives. *American Journal of Community Psychology, 39*(3/4), 239-253.

Homburg, A., & Stolberg, A. (2006). Explaining pro-environmental behavior with a cognitive theorie of stress. *Journal of Environmental Psychology, 26*(1), 1-14.

Homer, J. B., & Hirsch, G. B. (2006). System dynamics modeling for public health: Background and opportunities. *American Journal of Public Health, 93*(3), 452-458.

Hovland, C. I., Janis, I. L., & Kelley, H. H. (1953). *Communication and persuasion: Psychological studies of opinion change*. New Haven, CT: Yale University Press.

Howick, S., Ackermann, F., & Andersen, D. (2006). Linking event thinking with structural thinking: methods to improve client value in projects. *System Dynamics Review, 22*(2), 113-140.

Howick, S., Eden, C., Ackermann, F., & Williams, T. (2006). Building confidence in models for multiple audiences: the modelling cascade. *European Journal of Operational Research, 186*(3), 1068-1083.

Hu, L., & Bentler, P. M. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological Methods, 3*(4), 424-453.

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling, 6*(1), 1-55.

Hubig, C. (2003). Selbständige Nutzer oder verselbständigte Medien - Die neue Qualität der Vernetzung [Independent users or media becoming independent - the new quality of interconnection]. In F. Mattern (Ed.), *Total vernetzt. Szenarien einer informatisierten Welt* (pp. 211-229). Berlin: Springer.

IAF. (2006). *The biomonitoring futures project: Final report and recommendations*. Princeton: Institute for Alternative Futures.

ITU. (2005). *The Internet of Things. Executive Summary*. Geneva: ITU.

ITU. (2006). *digital.life*. Geneva: ITU.

Janis, I. L. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (Vol. 3, pp. 166-224). San Diego, CA: Academic Press.

Janz, N., & Becker, M. (1984). The health belief model - a decade later. *Health education quarterly, 11*(1), 1-47.

Jessup, L. M., & Robey, D. (2002). The relevance of social issues in ubiquitous computing environments. *Communications of the ACM, 45*(12), 88-91.

Johnson-Laird, P. N. (1983). *Mental models: Towards a cognitive science of language, inference and consciousness*. Cambridge, MA: Havard University Press.

Johnson-Laird, P. N. (2006). Models and heterogeneous reasoning. *Journal of Experimental and Theoretical Artificial Intelligence, 18*(2), 121-148.

Karger, C. R., & Wiedemann, P. M. (1998). Kognitive und affektive Komponenten der Bewertung von Umweltrisiken [Cognitive and affective components of the appraisal of environmental risks]. *Zeitschrift für Experimentelle Psychologie, 45*(4), 334-344.

Kasperson, J. X., Kasperson, R. E., Pidgeon, N., & Slovic, P. (2003). The social amplification of risk: assessing fifteen years of research and theory. In N. Pidgeon, R. E. Kasperson & P. Slovic (Eds.), *The social amplification of Risk* (pp. 13-46). Cambridge: Cambridge University Press.

Kasperson, R. E., Golding, D., & Tuler, S. (2005). Social distrust as a factor in siting hazardous facilities and communicating risks. In J. X. Kasperson & R. E. Kasperson (Eds.), *The Social Contours of Risk* (Vol. 1, pp. 29-50). London: Earthscan.

Kelly, G. A. (1955). *The psychology of personal constructs*. New York: Norton.

Kemp, R. (1993). Risikowahrnehmung: Die Bewertung von Risiken durch Experten und Laien - ein zweckmässiger Vergleich? [Risk perception: Assessment of risks by experts and laypersons - an appropriate comparison?]. In U. Becker & e. al. (Eds.), *Risiko ist ein Konstrukt: Wahrnehmungen zur Risikowahrnehmung* (pp. 109-127). München: Knesebeck.

Kitchin, R. M. (1994). Cognitive maps: What are they and why study them? *Journal of Environmental Psychology, 14*(1), 1-19.

Kivits, J. (2006). Informed patients and the Internet: A mediated context for consulations with health professionals. *Journal of Health Psychology, 11*(2), 269-282.

Kleinhückelkotten, S., & Neitzke, H.-P. (2009). Leben in der vernetzten Welt. Opportunities und Risiken allgegenwärtiger Informations- und Kommunikationstechnologien [Living in the interconnected world. Chances and risks of ubiquitous information and communication technologies]. *EMF-Monitor, 14*(2), 1-11.

Kruse, L. (1981). Psychologische Aspekte des technischen Fortschritts [Psychological dimensions of technological progress]. In G. Ropohl (Ed.), *Interdisziplinäre Technikforschung* (pp. 72-82). Berlin: Schmidt.

Kuttschreuter, M. (2006). Psychological determinants of reactions to food risk messages. *Risk Analysis, 26*(4), 1045-1057.

Kuttschreuter, M., & Gutteling, J. M. (2004a). Experience-based processing of risk information: The case of the millennium bug. *Journal of Risk Research, 7*(1), 3-16.

Kuttschreuter, M., & Gutteling, J. M. (2004b). Time will tell: changes in risk perception and the processing of risk information about the Y2K-risk. *Computers in Human Behavior, 20*(6), 801-821.

Langan-Fox, J., Code, S., & Langfield-Smith, K. (2000). Team mental models: Techniques, methods, and analytic approaches. *Human Factors, 42*(2), 242-271.

Lazarus, L. (1966). *Psychological stress and the coping process*. New York: McGraw-Hill.

Leach, J. (2003). Improving user security behavior. *Computers and Security, 22*(8), 685-692.

Lerner, J. S., & Keltner, D. (2001). Fear, anger, and risk. *Journal of Personality and Social Psychology, 81*(1), 146-159.

Leventhal, H. (1970). Findings and theory in the study of fear communication. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (Vol. 5, pp. 119-186). New York: Academic Press.

Leventhal, H., Diefenbach, M. A., & Leventhal, E. A. (1992). Illness cognition: Using common sense to understand treatment adherence and affect cognition interactions. *Cognitive Therapie and Research, 16*(2), 143-163.

Levine, R. L. (2000). *System dynamics applied to psychological and social problems*. Paper presented at the Proceedings of the 18th International Conference of the System Dynamics Society.

Levine, R. L. (2003). *Models of attitude and belief change from the perspective of system dynamics*. Paper presented at the Proceedings of the 21st International Conference of the System Dynamics Society.

Levine, R. L., & Doyle, J. K. (2002). *Modeling generic structures and patterns in social psychology*. Paper presented at the Proceedings of the 20th International Conference of the System Dynamics Society.

Levine, R. L., Van Sell, M., & Rubin, B. (1992). System dynamics and the analysis of feedback processes in social and behavioral systems. In R. L. Levine & H. E. Fitzgerald (Eds.), *Analysis of Dynamic Psychological Systems* (Vol. 1, Basic Approaches to General Systems, Dynamic Systems, and Cybernetics, pp. 145-266). New York: Plenum Press.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*(1), 71-90.

Linneweber, V. (2007). Menschen, Maschinen, Mobilität: Ein Essay über Potentiale von Fahrassistenzsystemen [Humans, machines, mobility: An essay on potentials of driver assistent systems]. *Umweltpsychologie, 11*(2), 128-137.

Little, T. D., Cunningham, W. A., Shahar, G., & Widaman, K. F. (2002). To parcel or not to parcel: Exploring the question, weighing the merits. *Structural Equation Modeling, 9*(2), 151-173.

Loewenstein, G. F., Weber, E. U., Hsee, C. K., & Welch, N. (2001). Risk as feelings. *Psychological Bulletin, 127*(2), 267-286.

Loroz, P. S., & Lichtenstein, D. R. (2004). The moderating role of perceived behavior-outcome covariation on consumer estimates of health risk. *Journal of Public Policy and Marketing, 23*(1), 54-64.

Lyon, D. (2001). Facing the future: Seeking ethics for everyday surveillance. *Ethics and Information Technology, 3*(3), 171-181.

MacCallum, R. C., & Austin, J. T. (2000). Applications of structural equation modeling in psychological research. *Annual Review of Psychology, 51*, 201-226.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy - a revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Martens, T. (2007). Handlungstypen als Grundlage für die Massschneiderung von umweltpsychologischen Informationen [Behavior types as the basis for tailoring environment psychological information]. *Umweltpsychologie, 2*(21), 69-87.

Martens, T., & Rost, J. (1998). Der Zusammenhang von wahrgenommener Bedrohung durch Umweltgefahren und der Ausbildung von Handlungsintentionen [The relation between perceived environmental threats and the buildung of intentions to act]. *Zeitschrift für Experimentelle Psychologie, 45*(4), 245-364.

Mattern, F. (2003). Vom Verschwinden des Computers - Die Vision des Ubiqutious Computing [From the disappearance of the computers - the vision of ubiqutious computing]. In F. Mattern (Ed.), *Total vernetzt, Szenarien einer informatisierten Welt* (pp. 1-41). Berlin: Springer.

Mattern, F. (2005). Ubiquitous computing: Scenarios for an informatized world. In A. Zerdick, A. Picot, K. Schrape, J.-C. Burgelman, R. Silverstone, V. Feldmann, C. Wernick & C. Wolff (Eds.), *E-Merging Media - Communication and the Media Economy of the Future* (pp. 145-163). Berlin: Springer.

Mattern, F., & Floerkemeier, C. (2010). Vom Internet der Computer zum Internet der Dinge [From the Internet computers to the Internet of things]. *Informatik-Spektrum, 33*(2), 107-121.

McCallum, D. B., Covello, V., & Peters, R. G. (1997). The determinants of trust and credibility in environmental risk communication. *Risk Analysis, 17*(1), 43-54.

McGinnis, J. M. (2001). Does proof matter? Why strong evidence sometimes yields weak actions. *American Journal of Health Promotion, 15*, 391-396.

McGuire, W. J. (1969). The nature of attitudes and attitude change. In G. Lindzey & E. Aronson (Eds.), *Handbook o social psychology* (Vol. 3, pp. 136-314). Reading, MA: Addison-Wesley.

Mehrabian, A., & Russell, J. A. (1974). *An approach to environmental psychology*. Cambridge, Mass.: MIT Press.

Meier, K. (2005). *Überall und unsichtbar [Everywhere and invisible]*. St. Gallen: Risiko-Dialog.

Meier, K. (2006). *Pervasive Computing im Dialog. Aussichten und Einsichten [Pervasive computing discussed. Insights and outlooks]*. St. Gallen: Stiftung Risiko-Dialog.

Meijnders, A. L., Midden, C. J. H., & Wilke, H. A. M. (2001a). Communications about environmental risks and risk-reducing behavior: The impact of fear on information processing. *Journal of Applied Social Psychology, 31*(4), 754-777.

Meijnders, A. L., Midden, C. J. H., & Wilke, H. A. M. (2001b). Role of negative emotion in communication about CO2 risks. *Risk Analysis, 21*(5), 955-966.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Moore, G. E. (1965). Cramming more components onto integrated circuits. *Electronics, 38*, 14-117.

Moore, G. E. (2003). *No exponential is forever: But "forever" can be delayed*. Paper presented at the Proceedings of the Solid-State Circuits Conference ISSCC.

Moore, M. M. (2003). Pillars of your community. *CSO online* Retrieved January 3, 2011, from http://www.csoonline.com/read/010903/pillars.html

Morgan, M. G., Fischhoff, B., Bostrom, A., & Atman, C. J. (2002). *Risk communication: A mental models approach*. Cambridge: Cambridge University Press.

Morse, J. M. (2000). Determining sample size. *Qualitative Health Research, 10*(1), 3-5.

Müller, G., Kreutzer, M., Strasser, M., Eymann, T., Hohl, A., Nopper, N., et al. (2003). Geduldige Technologie für ungeduldige Patienten: Führt Ubiquitous Computing zu mehr Selbstbestimmung? [Patent technology for impatient patents: Does ubiquitous computing increase self-determination?]. In F. Mattern (Ed.), *Total vernetzt, Szenarien einer informatisierten Welt* (pp. 159-186). Berlin: Springer.

Neitzke, H.-P., Behrendt, D., & Osterhoff, J. (2006). *Alltagsszenarien in der AACC-Welt [Scenarios of everyday living in an AACC-world]*. (AACCrisk Report 1/2006). Hannover: Ecolog-Institut.

Neitzke, H.-P., Calmbach, M., Behrendt, D., Kleinhückelkotten, S., Wegner, E., & Wippermann, C. (2008). Risks of ubiquitous information and communication technologies. *GAIA, 17*(4), 362-369.

Neitzke, H.-P., & Vedder, D. (2010). *Chancen nutzen, Risiken minimieren! Unser zukünftiger Umgang mit allgegenwärtigen Informations- und Kommunikationstechnologien [Profiting from chances, minimizing risks! Our future coping with ubiquitous information and communication technologies]*. Hanover: ECOLOG.

Nerb, J., Spada, H., & Wahl, S. (1998). Kognition und Emotion bei der Bewertung von Umweltschadensfällen: Modellierung und Empirie [Cognitions and emotions of the appraisal of environmental hazards: Modelling and empiricism]. *Zeitschrift für Experimentelle Psychologie, 45*(4), 251-269.

Neuhauser, L., & Kreps, G. L. (2003). Rethinking communication in the e-health era. *Journal of Health Psychology, 8*(1), 7-23.

Neuwirth, K., Dunwoody, S., & Griffin, R. J. (2000). Protection motivation and risk communication. *Risk Analysis, 20*(5), 721-734.

Newell, A., & Simon, H. A. (1972). *Human problem solving*. Englewood Cliffs (N.J.): Prentice-Hall.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Norman, D. A. (1983). Some Observations on Mental Models. In D. Gentner & A. L. Stevens (Eds.), *Mental Models* (pp. 7- 14). Hillsdale, New Jersey, London: LEA.

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory* (3nd ed.). New York: McGraw-Hill.

Opwis, K. (1985). *Mentale Modelle dynamischer Systeme: Analyse und Weiterführung methodischer Grundlage von psychologischen Experimenten zum Umgang von Personen mit Systemen. [Mental models of dynamic systems: Analysis and development of the methodological basis of psychological experiments on how people deal with systems].* Freiburg i.Br.

Pechmann, C., Zhao, G., Goldberg, M. E., & Reibling, E. T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing, 67*(2), 1-18.

Peter, U., & Kaufmann-Hayoz, R. (2000). The concept of control: A key concept in understanding and overcoming barriers to responsible environmental behavior. In W. J. Perrig & A. Grob (Eds.), *Control of Human Behavior, Mental Processes, and Conciousness* (pp. 307-322). Manwan, NY: Erlbaum.

Peters, E., Burraston, B., & Mertz, C. K. (2004). An emotion-based model of risk perception and stigma susceptiblity: cognitive appraisals of emotion, affective reactivity, worldviews, and risk perceptions in the generation of technological stigma. *Risk Analysis, 24*(5), 1349-1367.

Peters, E., Lipkus, I., & Diefenbach, M. A. (2006). The functions of affect in health communications and the construction of health preferences. *Journal of Communication, 56*, 140-162.

Pfister, H.-R., & Böhm, G. (2008). The multiplicity of emotions: A framework of emotional functions in decision making. *Judgment and Decision Making, 3*(1), 5-17.

Pidgeon, N., & Rogers-Hayden, T. (2007). Opening up nanotechnology dialogue with the publics: Risk communication or 'upstream engagement'? *Health, Risk and Society, 9*(2), 191-210.

Poldervaart, P. (2009). Wenn Etiketten das Recycling stören [When tags interfere with recycling]. *Umwelttechnik Schweiz, 12*(09), 3.

Poortinga, W., & Pidgeon, N. (2006). Exploring the structure of attitudes toward genetically modified food. *Risk Analysis, 26*(6), 1707-1719.

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers and Security, 26*(3), 229-237.

Powers, W. T. (1973). *Behavior: The control of perception*. New York: Aldine Publ.

Powers, W. T. (1990). Control theory: A model of organisms. *System Dynamics Review, 6*(1), 1-20.

Powers, W. T. (1991). Commentary on Bandura's 'human agency'. *American Psychologist, 46*(2), 151-153.

Prochaska, J. O., & DiClemente, C. C. (1986). Toward a comprehensive model of change. In W. R. Miller & N. Heather (Eds.), *Treating Addictive Behaviors: processes of change* (pp. 3-27). New York: Plenum.

Prochaska, J. O., DiClemente, C. C., & Norcross, J. C. (1992). In search of how people change: Applications to addictive behaviors. *American Psychologist, 47*(9), 1102-1114.

Prochaska, J. O., Norcross, J. C., & DiClemente, C. C. (2006). *Changing for good*. New York: Harper Collins.

Prochaska, J. O., & Velicer, W. F. (1997). The transtheoretical model of health behavior change. *American Journal of Health Promotion, 12*, 38-48.

Prochaska, J. O., Velicer, W. F., Rossi, J. S., Goldstein, M. G., Marcus, B. H., Rakowski, W., et al. (1994). Stages of change and decisional balance for 12 problem behaviors. *Health Psychology, 13*(3), 39-46.

Rassmussen, H. N., Wrosch, C., Scheier, M. F., & Carver, C. S. (2006). Self-regulation processes and health: The importance of optimism and goal adjustment. *Journal of Personality, 74*(6), 1721-1747.

Read, D., Bostrom, A., Morgan, M. G., Fischhoff, B., & Smuts, T. (1994). What do people know about global climate change? 2. Survey studies of educated laypeople. *Risk Analysis, 14*(6), 971-982.

Renn, O. (2005). *White paper on risk governance: Towards an integrative approach.* Geneva: International Risk Covernance Council.

Renn, O. (2008). Concepts of risk: An interdisciplinary review. Part 2: Integrative approaches. *GAIA, 17*(2), 196-204.

Renner, B., Schüz, B., & Sniehotta, F. F. (2008). Preventive health behavior and adaptive accuracy of risk perception. *Risk Analysis, 28*(3), 741-748.

Repenning, N. A. (2002). A simulation-based approach to understanding the dynamics of innovation implementation. *Organization Science, 13*(2), 109-127.

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influences on end users' information security practice behavior. *Computers and Security, 28*(8), 816-826.

Richardson, G. P. (1991). *Feedback thought in social science and systems theory*. Philadelphia: University of Pennsylvania Press.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52*(3), 596-604.

Rochford, E. B., & Blocker, T. J. (1991). Coping with 'natural' hazards as stressors. The prediction of activism in a flood disaster. *Environment and Behavior, 23*(2), 171-194.

Rogers, R. W. (1975). Protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. R. Cacioppo & R. E. Petty (Eds.), *Social Psychology: A sourcebook* (pp. 153-176). New York: Guilford.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of Health Behavior Research I: Personal and Social Determinants* (pp. 113-132). New York: Plenum Press.

Rohrschacher, H. (2002). *Intelligent and green?* Wien: Bundesministerium für Verkehr, Innovationen und Technologie.

Rouse, W. B., & Morris, N. M. (1986). On looking into the black-box: Prospects and limits in the search for mental models. *Psychological Bulletin, 100*(3), 349-363.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal, 19*(3), 122-131.

Sawyer, J. E., & Kernman, M. C. (1999). Responses to the Michelangelo computer virus threat: The role of information sources and risk homeostasis theory. *Journal of Applied Social Psychology, 29*(1), 23-51.

Scheier, M. F., & Carver, C. S. (2003). Goals and confidence as self-regulatory elements underlying health and illness behavior. In L. D. Cameron & E. A. Leventhal (Eds.), *The self-regulation of health and illness behavior* (pp. 17-39). New York/London: Routledge.

Schmidt, A. M., & Dolis, C. M. (2009). Something's got to give: The effect of dual-goal difficulty, goal progress, and expectancies on resource allocation. *Journal of Applied Psychology, 94*(3), 678-691.

Schoenberger, C. R. (2002). The Internet of things. *Forbes Magazine, 18*.

Schumacker, R. E., & Lomax, R. G. (2004). *A beginner's guide to structural equation modeling* (2nd ed.). Mahwah, NY: Lawrence Erlbaum.

Schütz, H., & Wiedemann, P. M. (2008). Framing effects on risk perception of nanotechnology. *Public understanding of science, 17*(3), 369-379.

Schwaninger, M., & Groesser, S. N. (2008). System dynamics as model-based theory building. *Systems Research and Behavioral Science, 25*(4), 447-465.

Schwaninger, M., & Pérez Rios, J. (2008). System dynamics and cybernetics: a synergetic pair. *System Dynamics Review, 24*(2), 145-174.

Sherman, D. K., Mann, T., & Updegraff, J. A. (2006). Approach/avoidance motivation, message framing, and health behavior: Understanding the congruency effect. *Motivation and Emotion, 30*(2), 164-168.

Siegrist, M. (2000). The Influence of trust and perceptions of risks and benefits on the acceptance of gene technology. *Risk Analysis, 20*(2), 195-203.

Siegrist, M., Cvetkovich, G., & Roth, C. (2000). Salient value similarity, social trust and risk/benefit perception. *Risk Analysis, 20*(3), 353-362.

Siegrist, M., Earle, T. C., Gutscher, H., & Keller, C. (2005). Perception of mobile phone and base station risks. *Risk Analysis, 25*(5), 1253-1264.

Siegrist, M., & Gutscher, H. (2006). Flooding risks: A comparison of lay people's perceptions and expert's assessments in Switzerland. *Risk Analysis, 26*(4), 971-979.

Siegrist, M., Keller, C., Kastenholz, H., Frey, S., & Wiek, A. (2007). Laypeople's and experts' perception of nanotechnology hazards. *Risk Analysis, 27*(1), 59-69.

Simonet, S., & Wilde, G. J. S. (1997). Risk: Perception, acceptance and homeostasis. *Applied Psychology: An International Review, 46*(3), 235-252.

Skinner, H. A., Maley, O., & Norman, C. D. (2006). Developing Internet-based ehealth promotion programs: The spiral technology action research (STAR) model. *Health Promotion Practice, 7*, 406 - 417.

Slovic, P. (1987). Perception of risk. *Science, 236*(280-285).

Slovic, P. (1992). Perception of risk: Reflections on the psychometric paradigm. In S. Krimsky & D. Golding (Eds.), *Social theories of risk* (pp. 117-152). Westport, Connecticut, London: Praeger.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2002). The affect heuristic. In T. Gilovich, D. Griffin & D. Kahneman (Eds.), *Heuristics and Biasses. The Psychology of Intuitive Judgement* (pp. 397-420). Cambridge, New York: Cambridge University Press.

Slovic, P., Finucane, M. L., Peters, E., & MacGregor, D. G. (2004). Risk as analysis and risk as feelings: Some thoughts about affect, reason, risk, and rationality. *Risk Analysis, 24*(2), 311-322.

Slovic, P., & Fischhoff, B. (1982). Targeting risks. *Risk Analysis, 2*(4), 227-234.

Slovic, P., Fischhoff, B., & Lichtenstein, S. (1982). Why study risk perception. *Risk Analysis, 2*(2).

Smith, M. (1989). Computer security-threats, vulnerabilities, and countermeasures. *Information Age, 11*(4), 205-210.

Som, C., Hilty, L., & Ruddy, T. (2004). The precautionary principle in the information society. *Human and Ecological Risk Assess, 10*(5), 787-799.

Spiekermann, S., & Rothensee, M. (2005). *Soziale und psychologische Bestimmungsfaktoren des Ubiquitous Computing [Social and psychological factors of ubiquitous computing]*. Berlin: Institut für Wirtschaftsinformatik, Humboldt-Universität zu Berlin.

Stajano, F. (2003). *Security for whom? The shifting security assumption of pervasive computing*. Berlin: Springer.

Stanton, J. M., Stam, K. R., Paul, M., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*, 124-133.

Statistisches Bundesamt Deutschland. (2007). 80-Prozent-Marke bei der Handy-Ausstattung überschritten [Adoption of mobile phones passed the 80% threshold]. Retrieved April 20, 2010, from http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Presse/pm/zdw/2007/PD07_019_p002.psml

Sterman, J. D. (2000). *Business dynamics systems thinking and modeling for a complex world*. Boston: McGraw-Hill.

Sterman, J. D. (2001). System dynamics modeling: Tools for learning in a complex world. *California Management Review, 43*(41), 8-27.

Stewart, A. (2004). On risk: Perception and direction. *Computers & Security, 23*(5), 362-370.

Stone, A. (2003). The dark side of pervasive computing. *Pervasive Computing, 2*(1), 4-8.

Strauss, A. L. (1999). *Qualitative analysis for social scientists* (Repr. ed.). Cambridge: Cambridge University Press.

Streiner, D. L. (2003a). Being inconsistent about consistency: When coefficient alpha does and doesn't matter. *Journal of Personality Assessment, 80*(3), 217-222.

Streiner, D. L. (2003b). Starting at the beginning: An introduction of coefficient alpha and internal consistency. *Journal of Personality Assessment, 80*(1), 99-103.

Tan, J. (2005). *E-health care information systems. An introduction for students and professionals*. San Francisco: Jossey-Bass.

Tautz, F. (2002). *E-Health und die Folgen. Wie das Internet die Arzt-Patienten-Beziehung und das Gesundheitssystem verändert. [E-health and its consequences. How the Internet changes the physician-patient relationship and the health system]*. Frankfurt: Campus.

Taylor, S. D., Bagozzi, R. P., Gaither, C. A., & Jamerson, K. A. (2006). The bases of goal setting in the self-regulation of hypertension. *Journal of Health Psychology, 11*(1), 141-162.

The Royal Society. (2006). *Digital healthcare: The impact of information and communication technologies on health and healthcare*. London: The Royal Society.

Thompson, D. C., Thompson, R. S., & Rivara, F. P. (2001). Risk compensation theory should be subject to systematic reviews of scientific evidence. *Injury Prevention, 7*(2), 86-88.

Thüring, M., & Jungermann, H. (1986). Constructing and running mental models for inferences about the future. In B. Brehmer, H. Jungermann, P. Lourens & G. Sevon (Eds.), *New Directions in the Research on Decision Making* (pp. 163-174). Amsterdam: North-Holand.

Tobias, R., & Mosler, H.-J. (2007). Einsatz der Computersimulation in der Umweltpsychologie [Using computer simulation in environmental psychology]. *Umweltpsychologie, 2*(21), 22-37.

Tolli, A. P. (2009). *Motivational and self-regulatory responses to interruptions.* University of Akron, Akron.

Trimpop, R. M. (1996). Risk homeostasis theory: Problems of the past and promises for the future. *Safety Science, 22*(1-3), 119-130.

Tsohou, A., Kikilakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gap. *Information Security Journal: A Global Perspective, 17*(5/6), 207-227.

Vancouver, J. B. (2005). The depth of history and explanation as benefit and bane for psychological control theories. *Journal of Applied Psychology, 90*(1), 38-52.

Vancouver, J. B., & Kendall, L. N. (2006). When self-efficacy negatively relates to motivation and performance in a learning context. *Journal of Applied Psychology, 91*(5), 1146-1153.

Vancouver, J. B., Putka, D. J., & Scherbaum, C. A. (2005). Testing a computational model of the goal-level effect: An example of a neglected methodology. *Organizational Research Methods, 8*(1), 100-127.

Vancouver, J. B., Thompson, C. M., Tischner, E. C., & Putka, D. J. (2002). Two studies examining the negative effect of self-efficacy on performance. *Journal of Applied Psychology, 87*(3), 506-516.

Vancouver, J. B., Thompson, C. M., & Williams, A. A. (2001). The changing signs in the relationships between self-efficacy, personal goals and performance. *Journal of Applied Psychology, 86*(4), 605-620.

Velicer, W. F., Norman, G. J., Fava, J. L., & Prochaska, J. O. (1999). Testing 40 predictions from the transtheoretical model. *Addictive Behaviors, 24*(4), 455-469.

Viswanath, K., & Kreuter, M. W. (2007). Health disparities, communication inequalities, and ehealth. *American Journal of Preventive Medicine, 32*(5), 131-133.

Waeger, P. A., Eugster, M., Hilty, L. M., & Som, C. (2005). Smart labels in municipal solid waste - a case for the precautionary principle? *Environmental Impact Assessment Review, 25*(5), 567-586.

Webb, T. L., & Sheeran, P. (2006). Does changing behavioral intentions engender behavior change? A meta-analysis of the experimental evidence. *Psychological Bulletin, 132*(2), 249-268.

Weiser, M. (1991). The computer for the 21st century. *Scientific American, 265*(3), 94-104.

Whitman, M. E. (2003). Enemy at the gate: Threats of information security. *Communications of the ACM, 46*(8), 91-95.

Wiebe, D. J., & Korbel, C. (2003). Defensive denial, affect, and the self-regulation of health threats. In L. D. Cameron & H. Leventhal (Eds.), *The Self-Regulation of Health and Illness Behavior* (pp. 184-203). London/New York: Routledge.

Wiener, N. (1948). *Cybernetics: Control and communication in the animal and machine*. Cambridge, MA: MIT Press.

Wilde, G. J. S. (1982a). Critical issues in risk homeostasis theory. *Risk Analysis, 2*(4), 249-258.

Wilde, G. J. S. (1982b). The theory of risk homeostasis: Implications for safety and health. *Risk Analysis, 2*(4), 209-225.

Wilde, G. J. S. (1998). Risk homeostasis theory: An overwiew. *Injury Prevention, 4*, 89-91.

Wippermann, C. (2007). *Wahrnehmung von Chancen und Risiken von IKT und AACC in den sozialen Milieus. Ergebnisse der qualitativen Analyse. [Perception of opportunities and risks of ICT and AACC in different social milieus. Results of qualitative analysis]. AACCrisk Report 2/2007*. Hannover: Ecolog.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communication Monographs, 61*(2), 113-134.

Witte, K. (1998). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In P. A. Andersen & L. K. Guerrero (Eds.), *Handbook of Communication and Emotion* (pp. 423-450). London: Academic Press.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campains. *Health Education Behavior, 27*(5), 591-615.

Wolstenholme, E. F. (2003). Towards the definition and use of a core set of archetypal structures in system dynamics. *System Dynamics Review, 19*(1), 7-26.

Workman, M. (2007). Gaining access with social engineering: an empirical study of the threat. *Information System Security, 16*(6), 315-331.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Wrosch, C., Miller, G. E., Scheier, M. F., & Brun de Pontet, S. (2007). Giving up on unattainable goals: Benefits for health? *Personality and Social Psychology Bulletin, 33*(2), 251-265.

Wrosch, C., Scheier, M. F., Carver, C. S., & Schulz, R. (2003). The importance of goal disengagement in adaptive self-regulation: When giving up is benefical. *Self and Identity, 2*(1), 1-20.

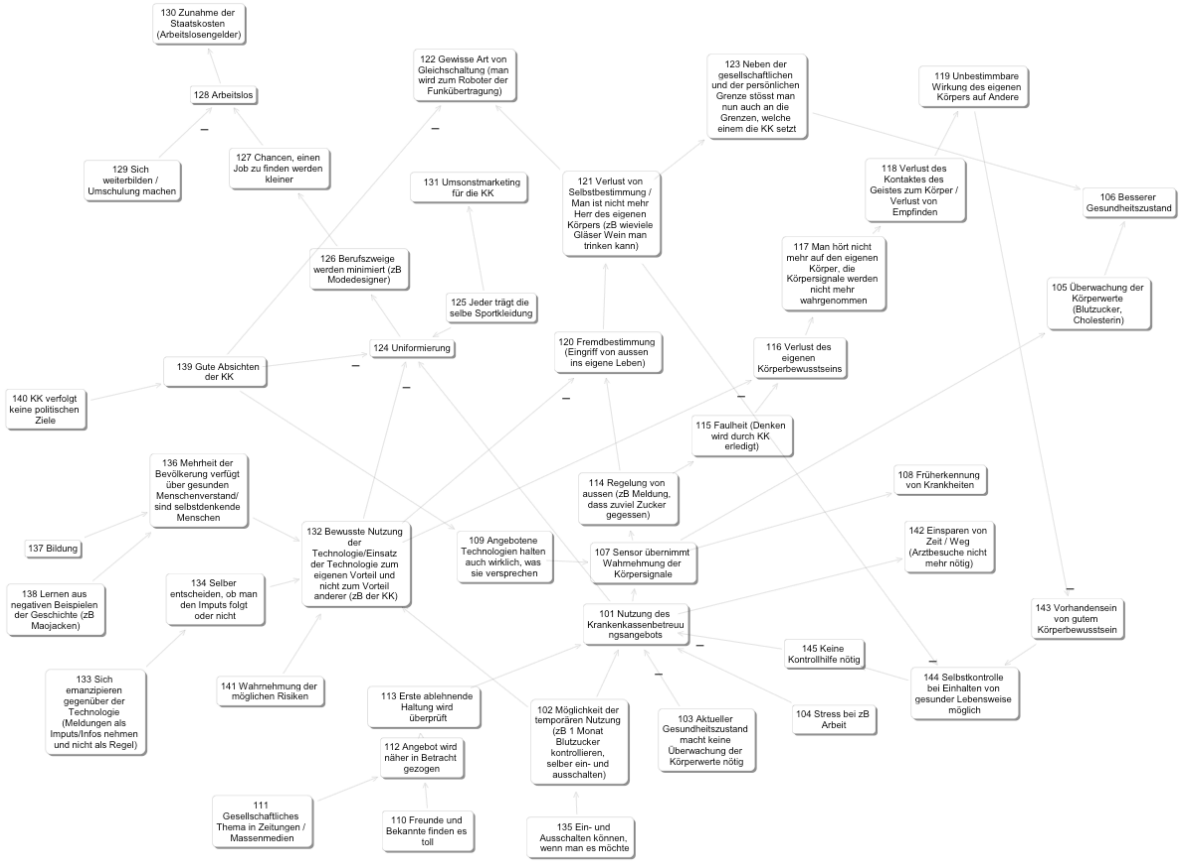
Wrosch, C., Scheier, M. F., Miller, G. E., Schulz, R., & Carver, C. S. (2003). Adaptive self-regualtion of unattainable goals: Goal disengagement, goal reengagement, and subjective well-being. *Personality and Social Psychology Bulletin, 29*(12), 1494-1508.

Young, R. M. (1983). Surrogates and mapping: Two kinds of conceptual models for interactive devices. In D. Gentner & A. L. Stevens (Eds.), *Mental Models* (pp. 35-52). London: Lawrence Erlbaum.

Appendix

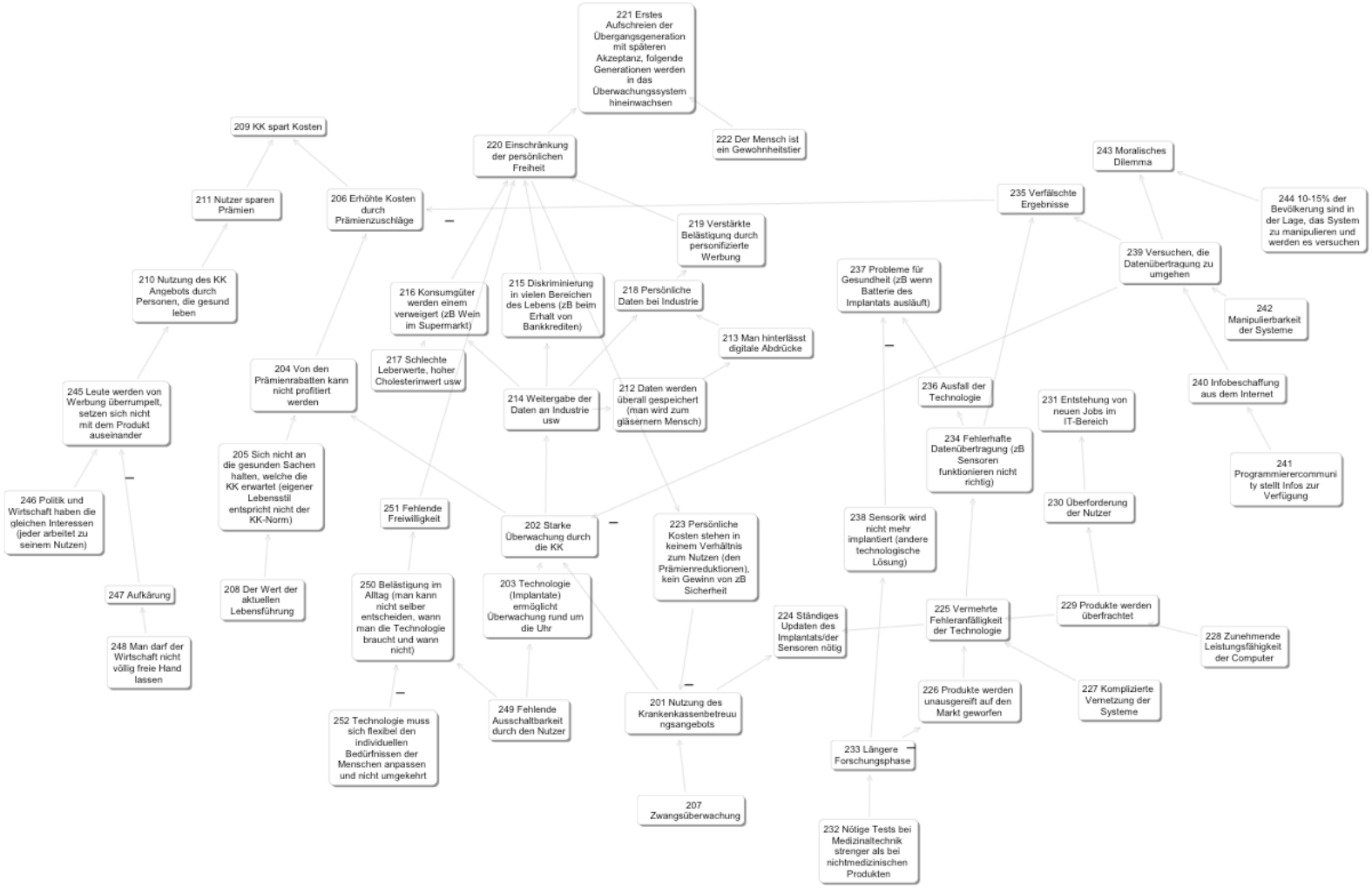
Appendix A: Individual Maps elicited in Study I

Preliminary note: The numbers of the concepts in the individual maps were renumbered prior to the data analysis. The concept numbers as shown here are composed as follows: The two last digits correspond to the original concept numbers, which follow the order in which they were mentioned during the interview. The first digit (or the first two, respectively) represents the identification number of the respondents.



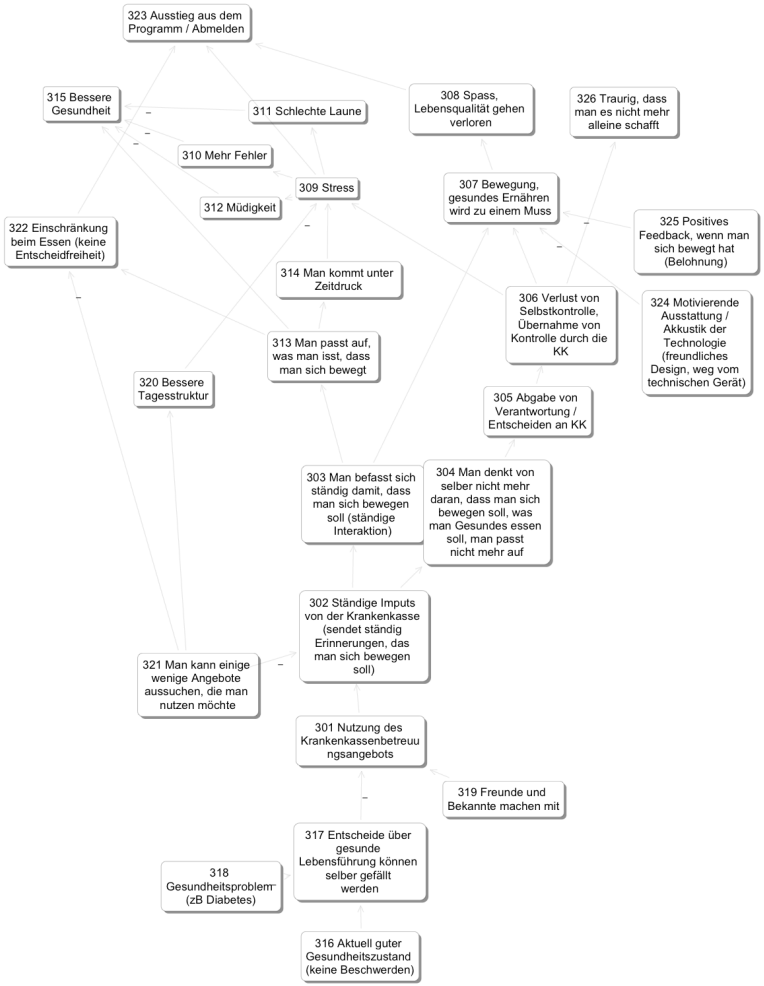
Individual Map of ‘Anne’, elicited on October 4, 2006

Appendix A: Individual Maps elicited in Study I (continued)

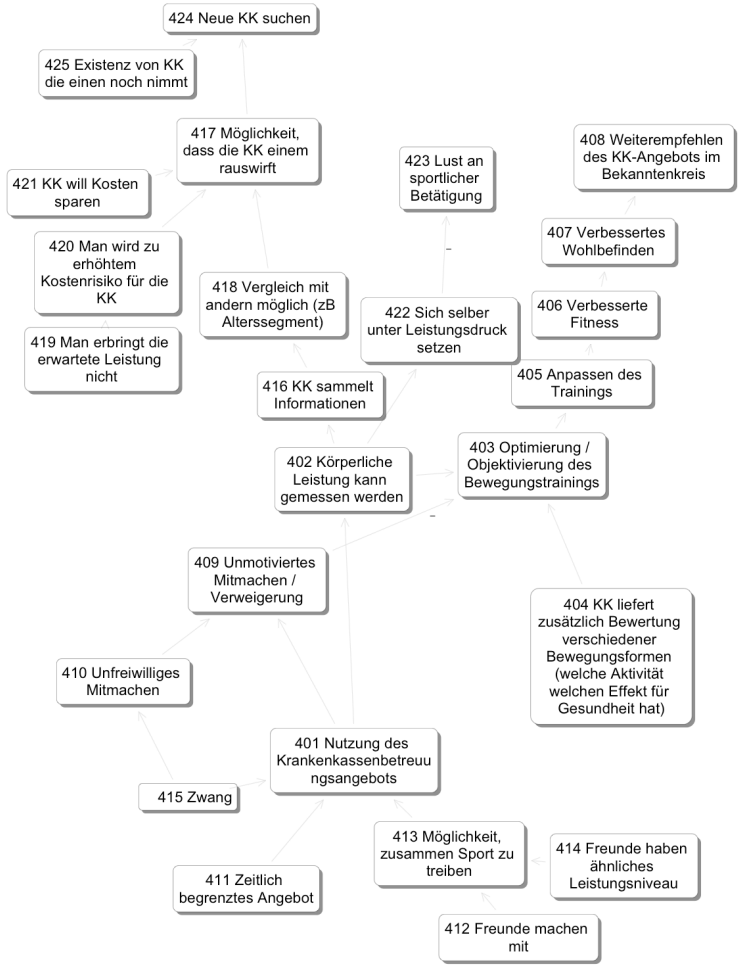


Individual Map of ‘Anthony’, elicited on October 5, 2006

Appendix A: Individual Maps elicited in Study I (continued)

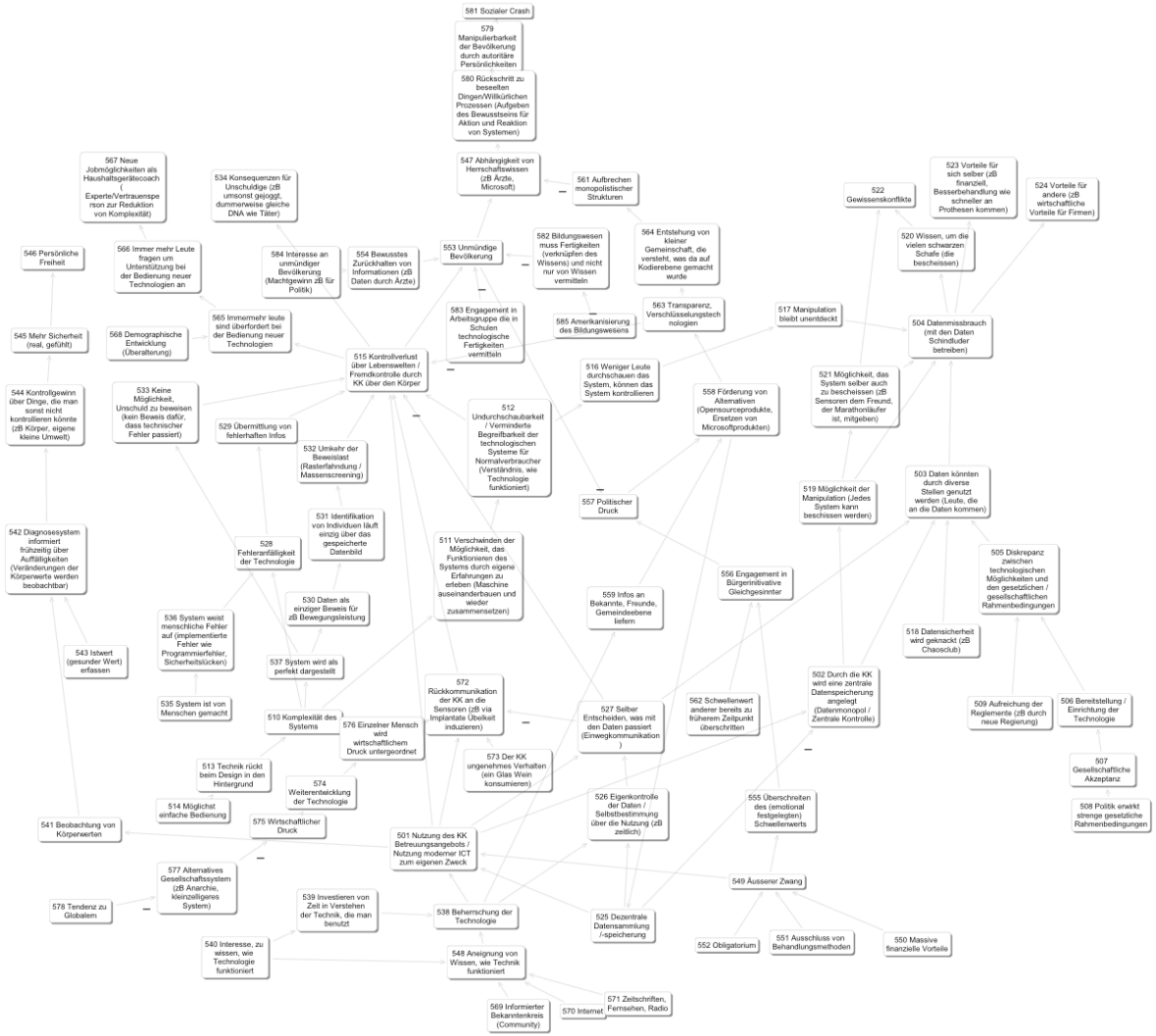


Individual Map of 'Cindy', elicited on October 5, 2006



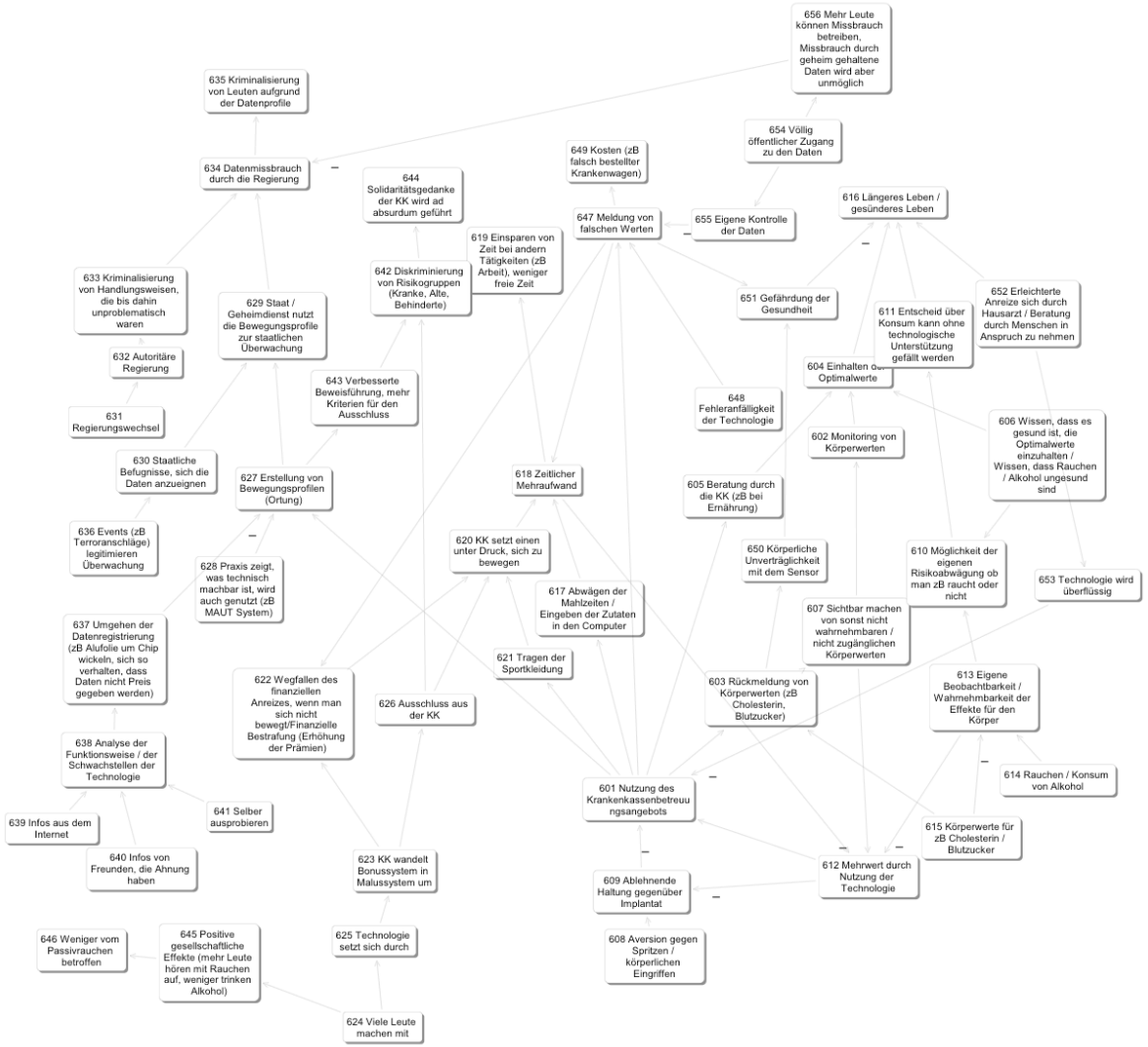
Individual Map of 'Marc', elicited on October 5, 2006

Appendix A: Individual Maps elicited in Study I (continued)



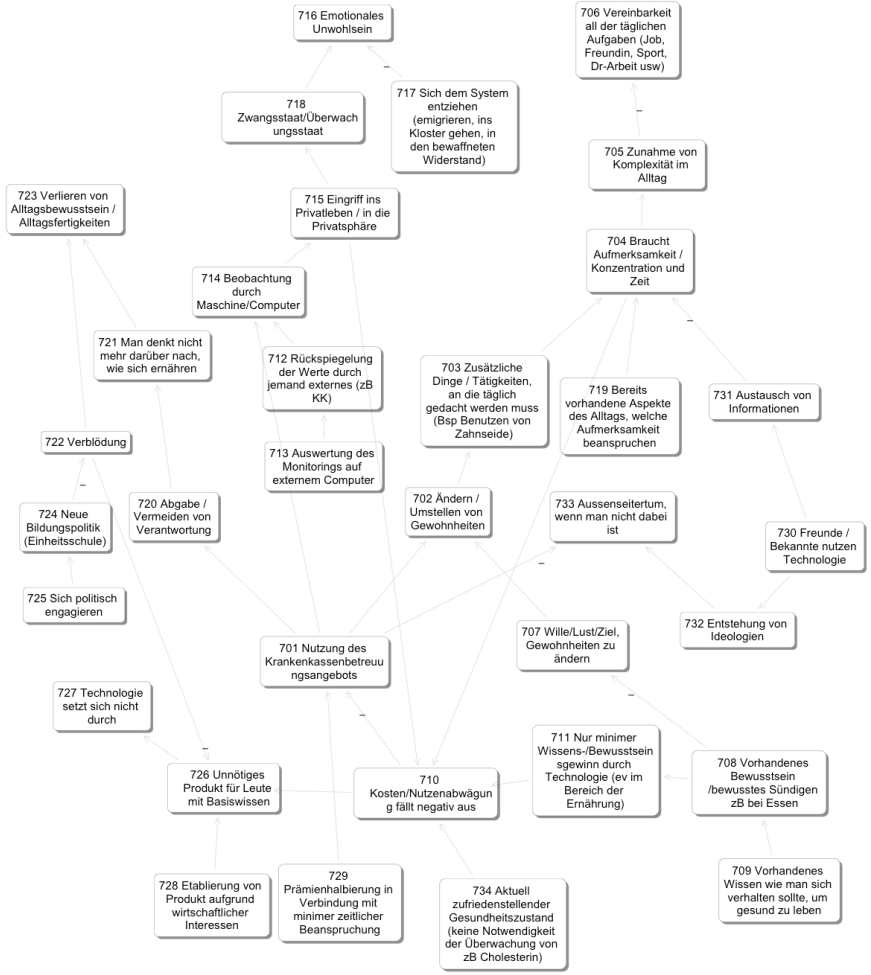
Individual Map of ‘Eric’, elicited on October 6, 2006

Appendix A: Individual Maps elicited in Study I (continued)

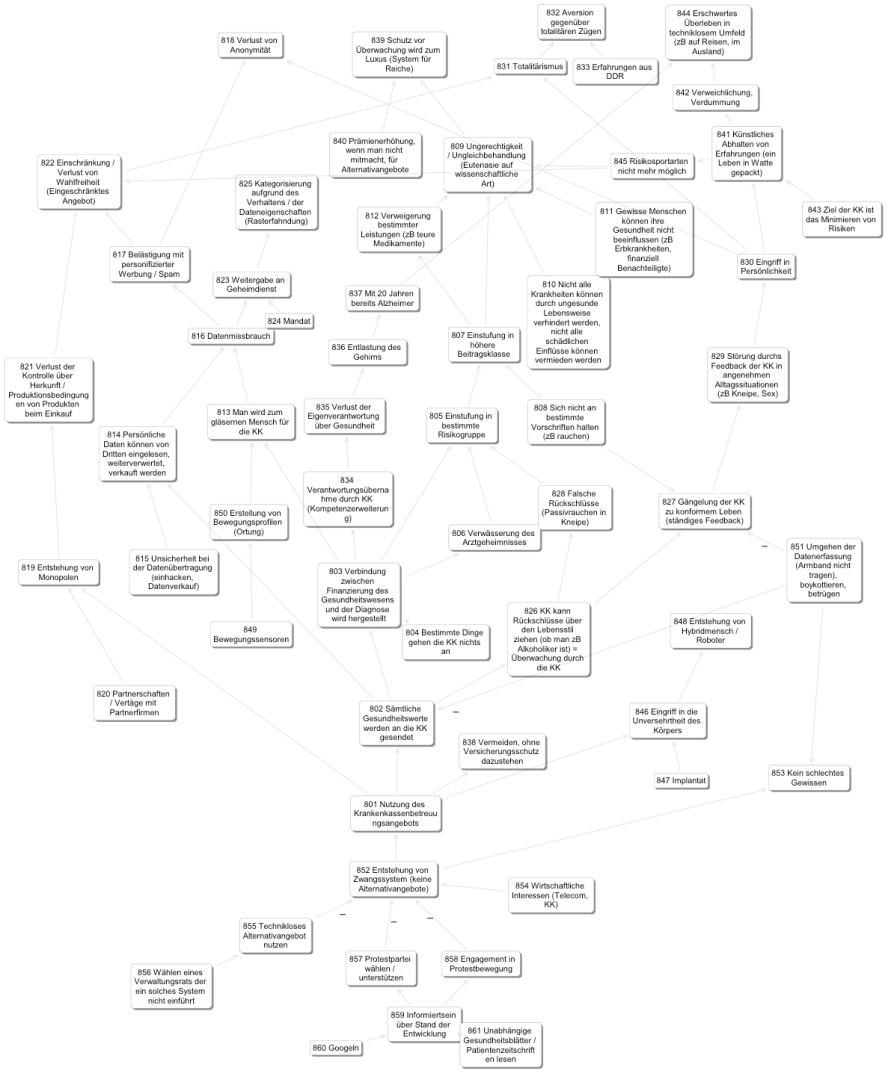


Individual Map of 'Ben', elicited on October 6, 2006

Appendix A: Individual Maps elicited in Study I (continued)

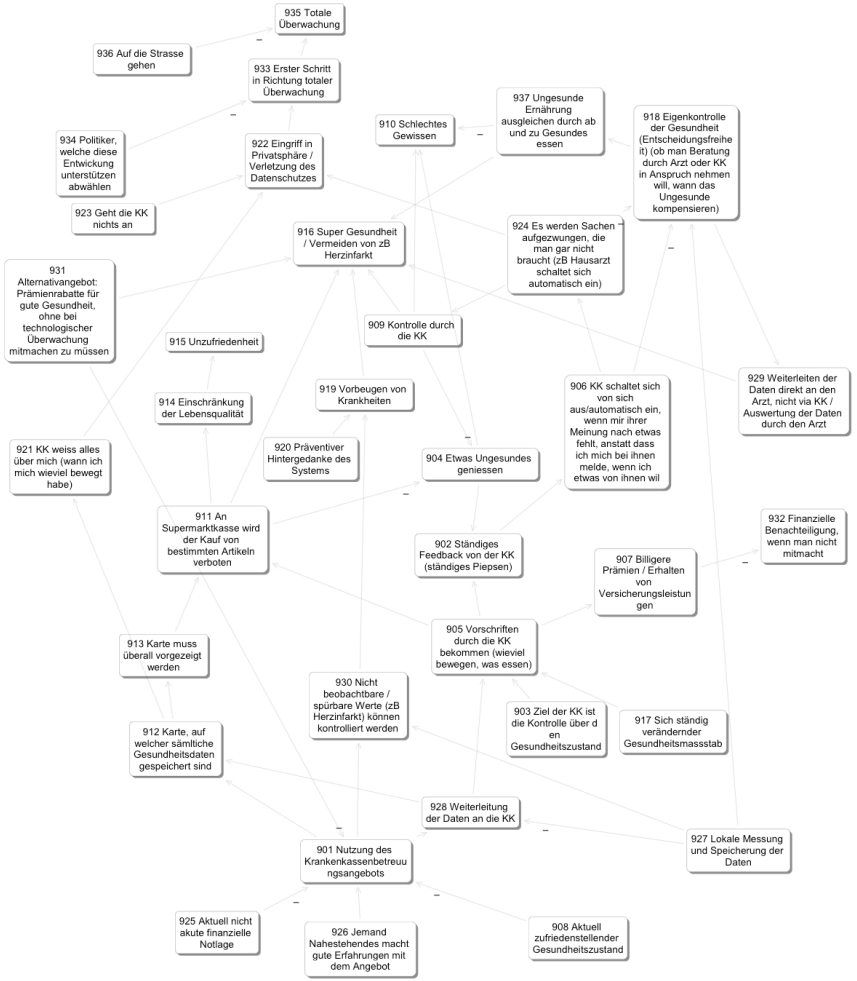


Individual Map of 'Michel', elicited on October 6, 2006

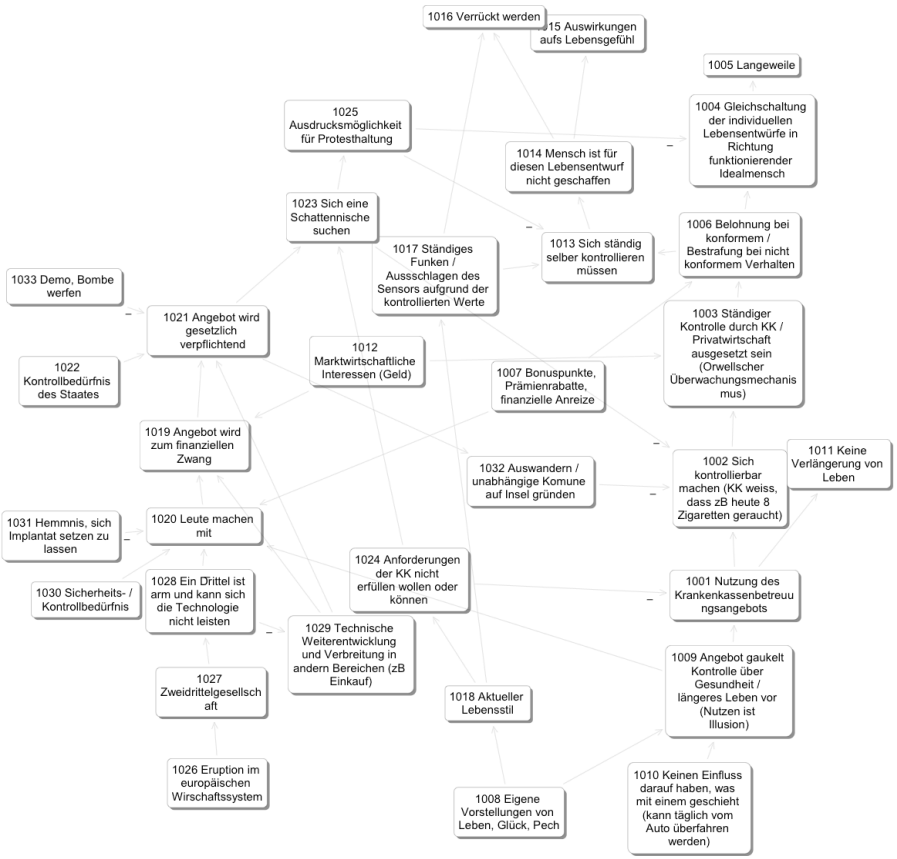


Individual Map of 'Helen', elicited on October 6, 2006

Appendix A: Individual Maps elicited in Study I (continued)

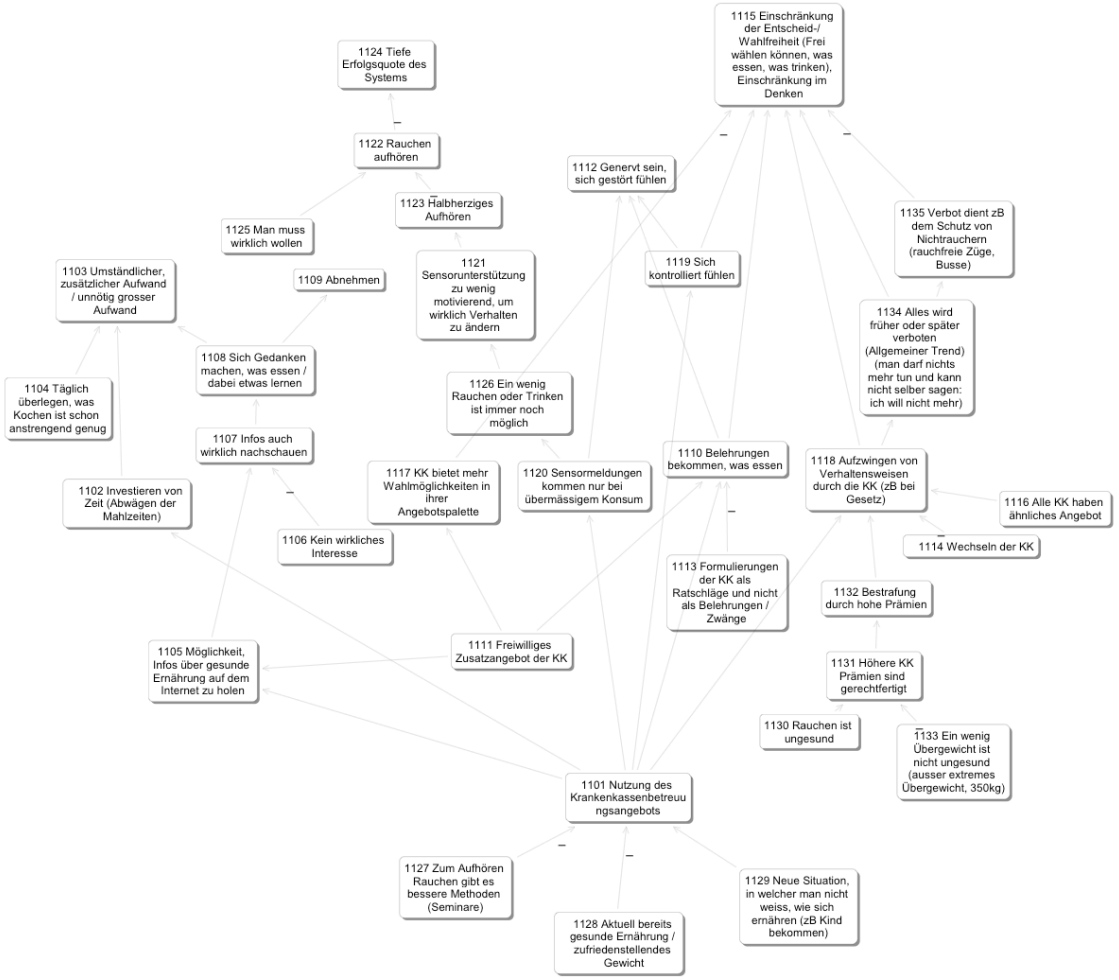


Individual Map of 'Neal', elicited on October 7, 2006



Individual Map of 'Bob', elicited on October 7, 2006

Appendix A: Individual Maps elicited in Study I (continued)



Individual Map of 'Donald', elicited on October 8, 2006

Appendix B: Overview of latent constructs, indicators and items

Latent construct	*Indicator*	*Item*
Previous experiences with ICT	Professional	'Which of the following information and communication technology applications do you use for your business?' (Desktop computer, laptop/notebook, ISDN telephone extension, DSL, Internet, telephone via Internet, VOIP, smart phone, Internet flat rate, W-LAN router, home server, e-mail, own website, mobile with Internet access, mobile with integrated camera, mobile with video telephone, USB stick/mp3 data stick, car navigation system) (repeated answer categories, total of 18 scores possible)
	Private	'Which of the following information and communication technology applications do you use privately?' (cf. question above) (repeated answer categories, total of 18 scores possible)
	Internet	'How often do you use the Internet at home?' 'How often do you use the Internet in your workplace?' 'How often do you use the Internet at school/at university?' 'How often do you use the Internet elsewhere (e.g., in an Internet corner)?' (5-point answer categories: 'never', 'fewer than several times per week', several times per week', 1-2 times per day', 'several times per day, actually all the time')
	Mobile phone	'How often do you use your mobile phone?' (5-point answer categories: 'never', 'fewer than several times per week', several times per week', 1-2 times per day', 'several times per day, actually all the time')
Introduction section two	It is imaginable that in the future ICT will be temporally and locally omnipresent: • ICT components (e.g., storage chips) will become increasingly smaller and will not be dependent on a specific location anymore. • They may be integrated within everyday objects such as textiles, electrical devices or food packages. From there they operate inconspicuously and nearly invisibly. • They can be interconnected wirelessly, gather information from their surroundings or exchange information among each other, as well as react accordingly by e.g., delivering information, regulating switches, control operations etc. There are different opinions concerning the chances and risks of temporally and locally omnipresent ICT. What do you think about it?	
Anticipated personal susceptibility	General	'My behavior will be observed.' 'Others can spy on what I do.'
	Health	'Due to the data storage, my patient rights are at risk.' 'If modern ICT permanently monitored my health state, I would feel externally controlled.' 'I suspect that the health insurer will know what I do in my leisure time.'
	Purchase	'I suspect that data about my shopping behavior will be handed to unauthorized persons.' 'I will be annoyed by an electronic shopping help.'
Institutional trust	Other institutions	'There will be controlling authorities who prevent data abuse.' 'Concerning the risks of modern ICT, I fully trust in consumer protection organizations'.
	Legislation	'I trust in our legislation to protect the citizens against data abuse.' 'The government will release laws to prevent hazards of future ICT.'
	Free market	'I fully trust in the organizations that collect sensitive data to responsibly deal with them.' 'Products which are ready for marketing are so soundly tested by the producer that their error rate is minimal.' 'Products who impede the user will not persist on the market.'

Appendix B: Overview of latent constructs, indicators and items (continued)

Latent construct	Indicator	Item
Benefits	Benefits 1	'Devices with key memory / automatic personalization will be easier to use'.
		'My interests will be better considered.'
		'We will be better informed.'
	Benefits 2	'Appliance of ubiquitous ICT will be more fun.'
		'The ubiquitous devices will be a part of me.'
		'Thanks to better connections, people will more easily contact each other.'
	Benefits 3	'I will have more opportunities.'
		'I will save time.'
		'Altogether, the worldwide interconnectedness will bring more advantages than disadvantages.'
Negative affect	Unease	'I have an uneasy feeling about what is approaching us.'
	Scare	'I am scared by the variety of ICT functions.'
Perceived threat	Ecological risks	'Because computers, scanners, chips, etc. require material, important resources will not be available anymore.'
		'Production, transportation and operation of ICT devices will create persistent environmental damages.'
		'The multitude of chips in products, devices and clothes will become garbage and consequently a big environmental burden.'
	Social risks	'Human behavior will be more and more controlled.'
		'The data collection will produce such a big amount of information that people will not be able to control it anymore.'
		'Due to the facilitated surveillance, people will not trust each other anymore.'
		'Due to the diffusion of the new ICT, profound personal relationships will become rare.'
		'People will rely on the technologies and consequently lose the skills/abilities to decide on their own.'
		'People who are not able to handle the ICT devices will be excluded.'
		'The increasing pervasion of our daily life with new ICT threatens our culture.'
		'In the future, we will be increasingly dependent on ICT.'
	General risks	'The future omnipresence and interconnectedness of ICT will provoke severe problems'
		'There is a risk that a technological breakdown will provoke irreversible damages.'
Introduction section three	In the following we are interested in what you believe the diffusion of temporally and locally omnipresent ICT will mean to you personally:	
Non-protective response	Overstrain	'In an everyday life which is pervaded by interconnected ICT I will be overstrained.'
	General denial	'Ubiquitous ICT will never exist.'
	Denial of personal susceptibility	'Potential risks of an everyday life pervaded by modern ICT will not affect me.'
	Helplessness	'We cannot do anything against the risks of new technologies'.

Appendix B: Overview of latent constructs, indicators and items (continued)

Latent construct	*Indicator*	*Item*
Intention to search for information	New developments	'I will continuously check on the developments in the field of interconnected ICT'
	Functioning	'I will check on the functioning of ICT supplies'
	Access	'I will check on who has access to the data stored by means of modern ICT.'
Perceived coping efficacy for information-seeking	Response efficacy	'I believe that checking on the developments and consequences of modern ICT is an appropriate action to lower their risks.'
	Self-efficacy	'I know how to find credible information on the development and consequences of modern ICT.'
Intention to take political actions	Pervasion of life	'I will take political actions against the pervasion of our life by modern ICT.'
	Avoid future risks	'If the risks of modern ICT increase, I will take political actions.'
Perceived coping efficacy for political action	Response efficacy	'I believe that taking political actions is an appropriate action to work against their risks.'
	Self-efficacy	'I am capable of taking political actions.'

Notes. If not otherwise mentioned, 4 -point scaled answer categories ('completely wrong', 'rather wrong', 'rather right', 'completely right'). Items were originally formulated in German and translated into English for the purpose of this publication.

Appendix C: Means, Standard Deviations, and Correlations of the Indicators

Indicator	*M*	*SD*	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*	*16*
1. Previous experiences (professional)	1.28	2.62	-															
2. Previous experiences (private)	3.50	3.52	.48	-														
3. Previous experiences (Internet)	0.62	.71	.57	.68	-													
4. Previous experiences (mobile)	2.11	1.42	.35	.54	.53	-												
5. Personal susceptibility (general)	3.00	.86	-.02	-.09	-.06	-.05	-											
6. Personal susceptibility (health)	2.67	.82	-.04	-.06	-.02	.01	.31	-										
7. Personal susceptibility (purchase)	2.98	.80	-.06	-.15	-.11	-.16	.39	.40	-									
8. Trust (other institutions)	2.60	.70	.06	.16	.13	.18	-.14	-.16	-.18	-								
9. Trust (legislation)	2.65	.72	.07	.14	.12	.19	-.16	-.19	-.19	.61	-							
10. Trust (free market)	2.63	.61	.09	.17	.17	.22	-.15	-.16	-.20	.55	.62	-						
11. Benefits 1	2.74	.73	.21	.40	.38	.44	-.11	-.09	-.21	.33	.38	.38	-					
12. Benefits 2	2.51	.69	.16	.37	.33	.41	-.09	-.04	-.19	.31	.32	.36	.73	-				
13. Benefits 3	2.70	.74	.24	.42	.41	.48	-.13	-.08	-.22	.34	.37	.40	.79	.74	-			
14. Negative affect (unease)	2.74	.95	-.19	-.35	-.30	-.29	.37	.31	.37	-.23	-.25	-.25	-.32	-.27	-.34	-		
15. Negative affect (scare)	2.49	1.00	-.22	-.44	-.38	-.38	.32	.18	.30	-.19	-.19	-.21	-.35	-.31	-.39	.55	-	
16. Threat appraisal (ecological risks)	2.68	.77	-.12	-.21	-.19	-.17	.27	.26	.33	-.15	-.16	-.16	-.14	-.12	-.18	.40	.33	-
17. Threat appraisal (social risks)	2.92	.59	-.13	-.30	-.23	-.24	.51	.40	.50	-.21	-.24	-.21	-.25	-.17	-.28	.60	.50	.54
18. Threat appraisal (general risks)	2.77	.71	-.14	-.29	-.21	-.23	.35	.33	.42	-.22	-.24	-.26	-.26	-.20	-.28	.49	.41	.56
19. NPR (overstrain)	2.48	.92	-.24	-.40	-.34	-.36	.22	.17	.26	-.14	-.14	-.16	-.27	-.22	-.30	.41	.48	.32
20. NPR (general denial)	2.26	.82	-.09	-.11	-.09	-.05	.04	.04	.08	.10	.07	.08	-.07	-.03	-.04	.11	.13	.08
21. NPR (denial of susceptibility)	2.33	.83	-.09	-.11	-.06	-.06	.01	-.03	-.02	.12	.16	.17	.06	.05	.03	.08	.13	.05
22. NPR (helplessness)	2.53	.85	-.12	-.14	-.12	-.10	.08	.08	.13	-.03	-.04	-.04	-.10	-.06	-.11	.17	.17	.12
23. Information (new developments)	2.21	.94	.28	.49	.45	.46	-.12	-.05	-.19	.25	.26	.31	.41	.41	.47	-.34	-.45	-.22
24. Information (functioning)	2.38	.97	.29	.50	.47	.46	-.09	-.02	-.15	.24	.26	.32	.43	.42	.49	-.32	-.44	-.21
25. Information (access)	2.52	1.02	.25	.41	.38	.40	.04	.10	-.01	.16	.17	.22	.34	.32	.39	-.17	-.30	-.08
26. Information (response efficacy)	2.81	.85	.20	.34	.29	.28	-.01	.01	-.05	.19	.19	.22	.35	.30	.37	-.19	-.26	-.06
27. Information (self efficacy)	2.52	.89	.30	.43	.39	.39	-.04	.00	-.08	.17	.16	.23	.36	.33	.39	-.28	-.35	-.14
28. Political action (pervasion of life)	1.63	.77	.07	.13	.16	.17	-.02	.07	-.05	.06	.06	.04	.06	.16	.08	0.00	-.03	.06
29. Political action (avoid future risks)	1.67	.81	.11	.14	.17	.16	.05	.10	.00	.01	-.01	.01	.05	.10	.07	.05	-.02	.05
30. Political action (response efficacy)	2.00	.87	.12	.10	.11	.05	.05	.04	.02	.01	.01	.01	.10	.10	.09	.02	.02	.09
31. Political action (self efficacy)	1.89	.86	.19	.19	.20	.14	.03	.01	-.02	-.02	.00	.03	.07	.07	.08	-.01	-.04	.00

Appendix C: Means, Standard Deviations, and Correlations of the Indicators (continued)

Indicator	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*	*27*	*28*	*29*	*30*
1. Previous experiences (professional)														
2. Previous experiences (private)														
3. Previous experiences (Internet)														
4. Previous experiences (mobile)														
5. Personal susceptibility (general)														
6. Personal susceptibility (health)														
7. Personal susceptibility (purchase)														
8. Trust (other institutions)														
9. Trust (legislation)														
10. Trust (free market)														
11. Benefits 1														
12. Benefits 2														
13. Benefits 3														
14. Negative affect (unease)														
15. Negative affect (scare)														
16. Threat appraisal (ecological risks)														
17. Threat appraisal (social risks)	-													
18. Threat appraisal (general risks)	.69	-												
19. NPR (overstrain)	.43	.43	-											
20. NPR (general denial)	.11	.12	.13	-										
21. NPR (denial of susceptibility)	.06	.02	.23	.20	-									
22. NPR (helplessness)	.22	.21	.23	.14	.10	-								
23. Information (new developments)	-.29	-.28	-.41	-.05	-.05	-.15	-							
24. Information (functioning)	-.26	-.26	-.41	-.06	-.07	-.16	.80	-						
25. Information (access)	-.09	-.09	-.27	-.08	-.07	-.15	.61	.70	-					
26. Information (response efficacy)	-.13	-.13	-.27	-.09	-.07	-.16	.43	.46	.45	-				
27. Information (self efficacy)	-.18	-.18	-.37	-.09	-.10	-.19	.51	.53	.50	.48	-			
28. Political action (pervasion of life)	-.04	.04	.01	.05	.06	-.03	.28	.29	.27	.09	.16	-		
29. Political action (avoid future risks)	.01	.06	-.03	.05	.03	-.09	.22	.18	.20	.07	.18	.50	-	
30. Political action (response efficacy)	.01	.06	-.05	-.03	-.01	-.11	.12	.12	.16	.26	.23	.28	.33	-
31. Political action (self efficacy)	-.05	-.01	-.12	-.03	-.03	-.16	.21	.22	.23	.17	.36	.39	.45	.51

Appendix D**:** Equations of the Mathematical Model of Individual Threat Control

1 **defensive motivation =** discrepancy*IF THEN ELSE(discrepancy<0,1,(100-Perceived Coping Efficacy)*0.01)[5]

2 **discrepancy =** perceived noncovered threat-Tolerated threat Threshold

3 **external impact on the perceived coping efficacy =** strength of the external impact on the perceived coping efficacy*
PULSE TRAIN(start time of the external impact on the perceived coping efficacy,
time duration of the external impact on the perceived coping efficacy, repeat time of the external impact on the perceived coping efficacy,
end of the external impact on the perceived coping efficacy)[6]

4 **external impact on the perceived overall threat =** initial perceived overall threat +
strength of the external impact on the perceived overall threat*PULSE(start time of the external impact on the perceived overall threat,
time duration of the external impact on the perceived overall threat)[7]

[5] The IF THEN ELSE-function returns the first value (in the second position in the parenthesis), if the condition (in the first position in the parenthesis) is true, and the second value (in the third position in the parenthesis), if the condition is false.

[6] PULSE TRAIN induces the strength of the external impact at the start time (in the first position in the parenthesis, over the time units specified in the second position in the parenthesis. The impact is repeated after the time units specified in the third position in the parenthesis. The repetition of the impact is stopped at the time unit specified in the last position in the parenthesis.

[7] The PULSE function operates by inducing the strength of the external impact at the start time (on the first position in the parenthesis), over the time units specified in the second position in the parenthesis.

5 **external impact on the tolerated threat threshold =** -1*strength of the external impact on the tolerated threat threshold*
PULSE(start time of the external impact on the tolerated threat threshold,
time duration of the external impact on the tolerated threat threshold)

6 **forgetting =** (Perceived Coping Efficacy-initial perceived coping efficacy)/time to forget

7 **Individual IS Security Behavior =** INTEG (net change in the individual IS security behavior, initial individual IS security behavior)

8 **net change in the individual IS security behavior =** IF THEN ELSE (protective motivation<0:AND:abs(protective motivation/
time to change the individual IS security behavior)>Individual IS Security Behavior, -Individual IS Security Behavior/
TIME STEP, protective motivation/time to change the individual IS security behavior)[8]

9 **net change in the perceived coping efficacy =** MIN((100-Perceived Coping Efficacy), (external impact on the perceived coping efficacy/
time to change the perceived coping efficacy-forgetting))[9]

10 **net change in perceived overall threat =** perceptual discrepancy/time to change perceived overall threat

11 **net change in the tolerated threat threshold =** IF THEN ELSE((defensive motivation +
external impact on the tolerated threat threshold)<0:AND:abs((defensive motivation + external impact on the tolerated threat threshold)
/time to change the tolerated threat threshold)>Tolerated Threat Threshold,-Tolerated Threat Threshold/TIME STEP,
(defensive motivation + external impact on the tolerated threat threshold)/time to change the tolerated threat threshold)

[8] The TIME STEP represents the integration interval chosen for the simulation. It is used in this equation to ensure that the reduction in Individual IS Security Behavior assumed non-negative values in the neighborhood of 0.

[9] The MIN function renders the smaller parameter of the two equations in the parenthesis.

12 **Perceived Coping Efficacy =** INTEG (net change in the perceived coping efficacy, initial perceived coping efficacy)

13 **Perceived Overall Threat =** INTEG (net change in the perceived overall threat, initial perceived overall threat)

14 **perceived noncovered threat =** SMOOTH(Perceived Overall Threat-Individual IS Security Behavior,
time to perceive the noncovered threat)[10]

15 **perceptual discrepancy =** external impact on the perceived overall threat-Perceived Overall Threat

16 **protective motivation =** discrepancy*IF THEN ELSE(discrepancy<0,1, Perceived Coping Efficacy*0.01)

17 **Tolerated Threat Threshold=** INTEG (net change in the tolerated threat threshold, initial tolerated threat threshold)

[10] The SMOOTH function approximates a simple first-order exponential moving average of the previous observations.

Curriculum Vitae

Stephanie Moser Froidevaux

Born 12th February 1978 in Biel, Switzerland

Education

2010 PhD in Psychology
University of Zurich, Switzerland, Faculty of Arts, Department of Psychology
Supervision: Prof. Dr. Hans-Joachim Mosler (Eawag)
Prof. Dr. Heinz Gutscher (University of Zurich)
Prof. Dr. Ruth Kaufmann-Hayoz (IKAOE)
Title: Risks of Ubiquitous Information and Communication Technologies: How Individuals Perceive, Cause, and Seek to Mitigate Them

2005 Licentiate in Psychology (lic.phil.hum.)
University of Berne, Switzerland, Faculty of Humanities, Department of Psychology
Major in social and general psychology, minor in general ecology and developmental psychology. MSc Thesis on water management in Latin America

2004 Field research within a NCCR North-South project in Bolivia, Latin America

2003 Internship at the Interdisciplinary Center for General Ecology (IKAOE) at the University of Berne, Switzerland

1998 Maturität: Type E, Wirtschaftsgymnasium Biel, Switzerland

Professional Experience

2010 Senior researcher, project management and management of a research group at the Interdisciplinary Center for General Ecology (IKAOE) at the University of Berne, Switzerland

2005-2010 Research Assistant at the IKAOE, operative project management

2003-2008 Health Instructor for Red Cross Immigrant's Courses

2005-2006 Administrative work in a center for asylum seekers with special health requirements

2002-2003 Administrative work in the asylum sector for the Red Cross Switzerland

1999 Workstay in Iceland

Other Activities

2006-2010	Contact person for the University of Berne with the association "Initiative Psychologie im Umweltschutz" (IPU Schweiz)
2007	Co-organisation of the 2nd IPU Congress in Berne
2005	Co-organisation of the Swiss Second Congress for Psychology Students (PSYKO) in Wattenwil, Switzerland
2003	Foundation and co-organisation of the Swiss First Congress for Psychology Students (PSYKO)
2006-2010	Family: two children

Publications (peer reviewed)

Moser, S., Bruppacher, S.E., & DeSimoni, F. (in press). Public Representation of Ubiquitous ICT Applications in the Outpatient Health Sector. *International Journal of Technology and Human Interaction.*

Moser, S., Bruppacher, S.E., & Mosler, H.-J. (2011). How people perceive and will cope with risks from the diffusion of ubiquitous information and communication technologies. *Risk Analysis, 31*(5), 832-846.

Moser, S., & Mosler, H.-J. (2008). Differences in influence patterns between adopter groups predicting the adoption of a solar disinfection technology for drinking water in Bolivia. *Social Science & Medicine 67*, 497–504.

Moser, S., Groesser, S.N., & Bruppacher, S.E. (in prep.). Managing Security Threats to Information Systems: A Dynamic Model of Controlling Individual Threats.

Conferences

Schlachter, I., Meloni, T., Lauper, E., & Moser, S. (2010). Behavior change in noise-producing activities – a model. Paper presented at the 1st EAA – EuroRegio 2010. Ljubljana, Slovenia.

Moser, S., Bruppacher, S.E., & Mosler, H.-J. (2009). How people perceive, and will cope with risks from an environment pervaded with ubiquitous ICT. Paper presented at the 8th Biennial Conference on Environmental Psychology. Zurich, Switzerland.

Moser, S., & Bruppacher, S.E. (2007). Risk perception of new information and communication technologies: An exploratory, qualitative approach to elicit lay people's mental models. Paper presented at the 7th Biennial Conference on Environmental Psychology. Bayreuth, Germany.

Moser, S., Mosler H.-J., & Heri S. (2005). Individual, social and environmental factors influencing the diffusion of a simple drinking water disinfection technology. Paper presented at the 6th Biennial Conference on Environmental Psychology. Bochum, Germany.